Escola Politècnica Superior
de Castelldefels
UNIVERSITAT POLITÈCNICA DE CATALUNYA

TREBALL DE FI DE CARRERA

TÍTOL DEL TFC: Optimització de servei d'una xarxa WiFi corporativa

TITULACIÓ: Enginyeria Tècnica de Telecomunicació, especialitat en Telemàtica

AUTOR: Adrià Homar i Pastor

DIRECTOR: Marco A. Peña Basurto

SUPERVISOR: Roc Messeguer Pallarès

DATA: 1 de Novembre de 2010

Títol: Optimització de servei d'una xarxa WiFi corporativa

Autor: Adrià Homar i Pastor

Director: Marco A. Peña Basurto

Data: 1 de Novembre de 2010

Resum

En aquest treball s'analitza una xarxa WiFi d'un centre universitari a partir de la base de coneixements tècnics de la carrera, i d'un aprofundiment teòric específic sobre la seguretat de la tecnologia, per tal d'extreure mesures correctives que permetin millorar l'estat i la qualitat del servei ofert a través d'aquesta xarxa.

Es realitza un abordatge doble que es manté durant la part principal del treball, en el qual es realitzen dues línies paral·leles que permeten la implementació de mesures correctives a curt termini i el disseny i integració d'una arquitectura de sistemes d'informació a llarg termini.

Aquest treball fa especial èmfasi en la seguretat de la tecnologia WiFi, per tal d'aportar robustesa i fiabilitat a la xarxa que permetin aconseguir el màxim temps de servei operatiu possible. Així doncs, l'enfocament dual es repeteix en una altra dimensió, on l'augment de la disponibilitat de la xarxa es troba en la intersecció de seguretat i millores tècniques. Aquests dos pilars han estat presents tant en les correccions tècniques com en la construcció de nous sistemes i procediments en el departament de tecnologies de la informació del centre.

Les recerca d'eines i sistemes d'informació és també una part integral d'aquest projecte. A través d'ells s'aconsegueix una major proactivitat en les tasques de manteniment i prevenció i resolució d'incidències, tenint aquesta millora un impacte enorme en la disponibilitat del servei.

És a través de la resolució del conjunt d'aspectes considerats en aquest treball que s'obté una millora real en l'experiència d'usuari de la xarxa.

Title: Corporate WiFi service optimization

Author: Adrià Homar i Pastor

Director: Marco A. Peña Basurto

Date: November, 1st 2010

Overview

This work analyzes a university WiFi network from the technical knowledge base of the degree, and going specifically deeper into the theoretical security of the technology to infer corrective measures to improve the status and quality of service offered through the network.

A dual approach is maintained during the main part of the work, in which there are two parallel lines that allow the implementation of corrective measures in the short term and the integration of design and architecture of specific information systems over time.

This work places emphasis on the safety of WiFi technology in order to provide robustness and reliability that allows the network to achieve the maximum possible operating uptime. Thus, the dual approach is repeated in another dimension, where the increased availability of the network is at the intersection of safety and technical improvements. These two pillars have been present in both the technical corrections as in the construction of new systems and procedures in the department of information technology of the center.

The research of tools and information systems is also an integral part of this project. Through them, more proactivity is achieved in preventive maintenance tasks and problem solving, taking such a huge impact on improving service availability.

It is through the resolution of all aspects considered in this work that a real improvement in the user experience of the network is obtained.

ÍNDEX

INTRODUCCIÓ

La aparició de la tecnologia sense fils WiFi ha permès la connectivitat LAN i l'accés a Internet d'una manera lliure i des d'una ubicació flexible. Comerços i emplaçaments públics fan ús de la tecnologia per a disposar d'una zona en la que clients i usuaris puguin connectar-se a Internet. En els primers, s'ofereix la connexió com un servei gratuït que impulsa i complementa l'activitat principal.

En el cas concret dels centres educatius, poder oferir WiFi als estudiants és també un servei afegit, que en el seu ús presenta dues vessants: l'acadèmica, ja que permet la recerca per Internet i la connexió als recursos educatius que el centre posi a disposició dels alumnes, i la d'un servei personal, en la que els estudiants poden treure partit als recursos disponibles a Internet. Això és especialment atractiu per als estudiants d'intercanvi, que constitueixen un perfil d'usuari que sovint necessita Internet per a comunicar-se.

Aquest TFC es desenvolupa en un centre educatiu privat de formació superior. Aquest ofereix l'accés a Internet en espais de lliure accés als alumnes, a través d'ordinadors fixes. Amb l'aparició de WiFi, es va voler donar també aquest servei a tot l'edifici, ja que era d'utilitat a dins les classes i complementava la oferta d'accés a Internet en poder utilitzar els equips propis amb llibertat d'ubicació.

Aquest treball està dividit en dos grans blocs. El primer, fins al final del capítol 4, conté: les valoracions inicials on es plantegen els objectius del projecte, els costos i la planificació, la base teòrica en els capítols 2 i 3, i culmina amb l'anàlisi de la xarxa objecte d'estudi en el capítol 4, que es tanca amb un replantejament de les valoracions inicials.

El segon bloc està composat pel disseny i la implementació de correccions en els capítols 5 i 6 respectivament, i per la valoració i conclusions del treball en els últims dos capítols.

1. CAPÍTOL 1. VALORACIONS INICIALS

En aquest capítol es planteja el treball partint d'una motivació i uns requeriments, a partir del quals es defineixen uns objectius que es desenvoluparan mitjançant unes tasques que es duran a terme en un temps i amb uns costos econòmics planificats.

1.1 Motivació

Aquest treball fi de carrera parteix d'un entorn real en el que una institució acadèmica de Barcelona pateix d'interrupcions en el servei de la xarxa WiFi que dóna servei en la seves instal·lacions. L'autor d'aquest treball presta actualment els seus serveis com a professional independent en el departament de tecnologies de la informació. Aquest treball doncs, serà un exercici que es durà terme en temps real al centre i que tindrà un impacte concret i mesurable.

Arribat el moment de finalitzar els estudis amb el treball de fi de carrera, poder treballar en la seguretat d'una tecnologia tan plenament present com WiFi en un entorn real, és una oportunitat d'aprofundir en quelcom molt interessant i amb molt bona projecció professional.

1.2 Requeriments

La xarxa WiFi d'aquesta institució presenta un problema greu de disponibilitat. El servei s'interromp i es desconeixen els motius que ho causen.

Segons la ISO/IEC 17799:2000 (Codi de Bones Pràctiques per a la Gestió de la Seguretat dels Sistemes de Informació) la disponibilitat és la garantia que els usuaris autoritzats tenen accés quan ho requereixin a la informació i els seus actius associats.

Per tal de millorar aquesta disponibilitat, s'abordarà el problema des de dos fronts. El primer serà el de seguretat, que contempla la disponibilitat com un dels seus pilars. El segon estarà orientat a obtenir aquelles millores tècniques que tinguin un impacte sobre la disponibilitat.

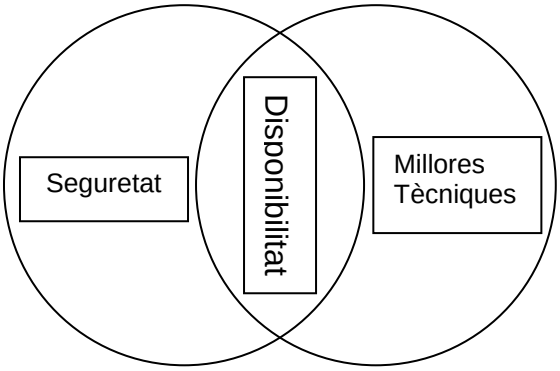

Fig. 1.1 Intersecció de la disponibilitat entre seguretat i millores tècniques

1.3 Objectius

O1. Ampliar la formació sobre la seguretat WiFi per tal d'obtenir els coneixements que constitueixin una base teòrica.

O2. Aprendre conceptes bàsics d'auditoria tècnica de seguretat, per tal de poder abordar l'anàlisi de la xarxa en qüestió des d'aquesta perspectiva.

O3. Cercar, avaluar i seleccionar les eines de treball apropiades.

O4. Analitzar la xarxa WiFi objecte d'estudi.

O5. Transmetre una base de coneixement de la tecnologia al departament de TI del centre aplicada a la seva xarxa WiFi i orientada a millorar el servei.

O6. Dissenyar i executar la implementació de mesures correctives sobre la xarxa que permetin augmentar la disponibilitat de la xarxa i minimitzar el temps d'aturada.

O7. Valorar les millores efectuades i proposar línies futures d'actuació.

1.4 Planificació aproximada

A continuació es detalla una planificació inicial del projecte que serà revisada posteriorment, un cop s'hagi dut a terme l'anàlisi de la xarxa (O4) i es disposi de més coneixement per a refinar els objectius del treball.

1.4.1 Llista de tasques

A continuació hi ha una llista de tasques amb la dedicació prevista. A la meitat del TFC i un cop assentada la base teòrica i analitzada la xarxa, es refinaran les tasques de la segona meitat.

- Estudi de la tecnologia WiFi. **70 hores.**
  - Estudi intensiu de la seguretat en WiFi. Història i solucions actuals. Objectius, mètodes i estat actual de les tècniques actuals.
  - Estudi i classificació de vulnerabilitats i atacs.

- Aproximació a la auditoria tècnica de seguretat. **30 hores**.
  - Cerca de documentació i estudi de manuals d'auditoria de seguretat existents, per tal d'extreure un procediment d'anàlisi.

- Cerca i avaluació d'eines. **20 hores**
  - Cerca i selecció d'eines per a l'anàlisi de xarxes WiFi
  - Cerca i selecció d'eines pel manteniment de xarxes WiFi

- Anàlisi. **40 hores.**
  - Estudi *in situ* de la xarxa WiFi corporativa. Estudi de l'emplaçament i de la topologia de xarxa. Presa de mesures del medi ràdio. Anàlisi dels equips de xarxa. Anàlisi de tràfic. Avaluació de seguretat.
  - Identificació de millores.

- Refinament d'objectius, tasques pendents i planificació. **4 Hores**.

- Disseny d'accions correctives. **20 hores**

- Implementació de les mesures dissenyades. **80 hores**.

- Valoració dels resultats i estudi de línies futures. **8 hores**.

El total de dedicació previst per a la realització del treball és de **272 hores**.

1.4.2 Calendari previst

La dedicació prevista per al treball és de dues hores els dies laborables. Així mateix, s'ha tingut en compte altres factors com les vacances (una setmana per Setmana Santa i dues a l'agost). A partir de l'esforç necessari comptabilitzat a l'anterior apartat, s'ha projectat el següent diagrama de Gantt:

Id	Nombre de tarea	Trabajo	Duración	Prede
1	**Estudi WiFi**	**70 h**	**37,47 d**	
2	Estudi inicial	30 h	30 h	
3	Estudi restant	40 h	44,94 h	2
4	Auditoria	30 h	30 h	3
5	**Eines**	**20 h**	**67,23 d**	
6	Eines Anàlisi	5 h	45,45 h	2
7	Eines Manten.	15 h	15 h	6
8	Anàlisi	40 h	40 h	1;4;6
9	Refinament	4 h	4 h	8
10	Disseny	20 h	20 h	9;7
11	Implementació	80 h	80 h	10
12	Valoració i futur	8 h	8 h	11

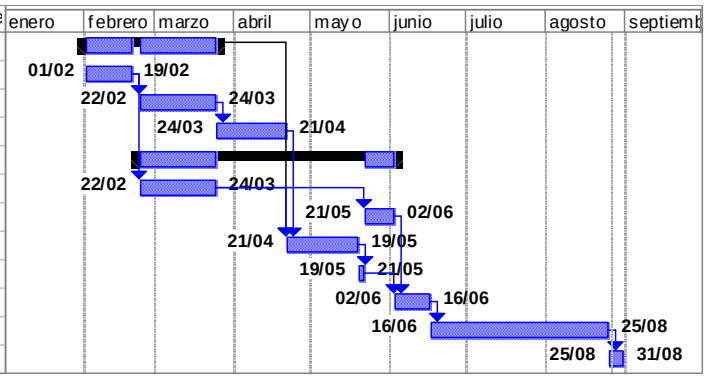

Fig. 1.2 Diagrama de Gantt de la planificació del treball

En el diagrama superior es pot veure l'esquema de prerequisits. L'estudi WiFi i la cerca d'eines d'anàlisi es realitzen simultàniament després d'un estudi inicial, en ser dos temes vinculats.

1.4.3 Estimació econòmica

Per tal de efectuar un càlcul dels costos del projecte, es necessita un preu / hora de treball. En aquest TFC no es preveuen costos de material de cap tipus, ja que tot el material amb el que es treballa es propietat del client. Per a determinar aquest preu, hem considerat una mitjana entre el preu de mercat d'un tècnic i el preu d'un estudiant en pràctiques. Per un projecte d'aquestes dimensions, 20 € / h s'ha considerat un preu adequat tenint en compte els preus de mercat actuals per a una feina d'aquesta durada i característiques. Pel que fa al preu / hora d'un estudiant, 6 € / h es troba adient. Per tant, el càlcul és:

Preu mig: (20 + 6) / 2 = 13 € / h

I, a partir de la dedicació:

Estimació econòmica: 272 hores x 13 € / h = **3.536 €**

Que es distribueixen de la següent manera:

Id	Nombre del recurso	Trabajo	Detalles	febrero	marzo	abril	mayo	junio	julio	agosto
1	Adrià	272 h	Costo	520,00 €	592,12 €	442,00 €	546,00 €	572,00 €	572,00 €	291,87 €
			Trabajo	40h	45,55h	34h	42h	44h	44h	22,45h
	Estudi inicial	*30 h*	Costo	390,00 €						
			Trabajo	30h						
	Estudi restant	*40 h*	Costo	115,70 €	404,29 €					
			Trabajo	8,9h	31,1h					
	Auditoria	*30 h*	Costo		137,13 €	252,87 €				
			Trabajo		10,55h	19,45h				
	Eines Anàlisi	*5 h*	Costo	14,30 €	50,70 €					
			Trabajo	1,1h	3,9h					
	Eines Manten.	*15 h*	Costo				163,13 €	31,87 €		
			Trabajo				12,55h	2,45h		
	Anàlisi	*40 h*	Costo			189,13 €	330,87 €			
			Trabajo			14,55h	25,45h			
	Refinament	*4 h*	Costo				52,00 €			
			Trabajo				4h			
	Disseny	*20 h*	Costo					260,00 €		
			Trabajo					20h		
	Implementació	*80 h*	Costo					280,13 €	572,00 €	187,87 €
			Trabajo					21,55h	44h	14,45h
	Valoració i futur	*8 h*	Costo							104,00 €
			Trabajo							8h

Fig. 1.3 Distribució d'hores i costos

2. CAPÍTOL 2. AUDITORIA DE SEGURETAT I TECNOLOGIA WIFI

Un cop plantejat el treball, aquest capítol assenta les bases teòriques recorrent les disciplines sobre les que es desenvoluparan les millores del servei: la auditoria tècnica de seguretat i la tecnologia WiFi.

2.1 Conceptes generals d'auditoria tècnica de seguretat

2.1.1 Definicions

Donat que el terme auditoria, en provenir del mon financer, en la seva aplicació a la seguretat dels sistemes d'informació no té una única definició consensuada, en aquest apartat es recullen les definicions que s'utilitzen en aquest treball. On es produeix una major necessitat de discerniment és entre els termes avaluació i auditoria de seguretat (*assessment* i *audit*) ja que en molts documents que es troben a Internet es poden trobar com a sinònims (i.e *Implementing a Successful Security Assessment Process del SANS*).

Una auditoria de sistemes d'informació és el procés de recollir i avaluar evidències per tal de determinar si un sistema d'informació salvaguarda els actius, manté la integritat de les dades, assoleix els objectius eficaçment i consumeix recursos eficientment.

Un auditoria de seguretat és una avaluació sistemàtica de la seguretat dels sistemes d'informació d'una companyia a través de mesurar el compliment d'un conjunt de criteris establerts, que té com a resultat en un registre factual, a través de proporcionar avaluacions tècniques independents i mesurables de les polítiques, procediments, estàndards, mesures i pràctiques de una organització per a tal de salvaguardar la informació electrònica de la seva pèrdua, dany, revelació no intencionada, o denegació de disponibilitat, de forma manual o sistemàtica.

Una avaluació de seguretat és el procés de determinar la efectivitat d'una entitat (equip, sistema, xarxa, procediment, persona, d'ara endavant objecte de la avaluació) complint objectius específics de seguretat. Les diferents avaluacions s'agrupen en tres mètodes: provar (*testing*), examinar i entrevistar. Els resultats de la avaluació s'empren per a determinar l'efectivitat dels controls de seguretat al llarg del temps.

Provar és el procés de exercitar un o més objectes de la avaluació sota condicions especifiques per tal de comparar comportaments actuals i esperats. Examinar és el procés de verificar, inspeccionar, revisar, observar, estudiar o analitzar un o més objectes de la avaluació per tal de facilitar la comprensió, clarificació o la obtenció de proves. Entrevistar és el procés de mantenir un

col·loqui amb persones individuals o grups dintre d'una organització per tal de facilitar la comprensió, clarificació, o identificar la ubicació de proves.

Les avaluacions manuals inclouen entrevistes al personal, escaneigs de vulnerabilitats, revisions dels controls d'accés a les aplicacions i als sistemes operatius, i l'anàlisi del accés físic als sistemes, entre d'altres. Les avaluacions automàtiques (CAAT) inclouen la generació d'informes d'auditoria per part del sistema o la utilització de *software* per a seguiment i control de canvis a arxius i configuracions.

Els resultats d'aquestes avaluacions estan generalment dirigides a la direcció de la organització, entitats legislatives, altres auditors, o el públic.

Ira Winkler, president del ISAG, defineix senzillament una auditoria com "una avaluació d'un determinat estàndard" i diu sobre les avaluacions:

- Són un intent lliure de localitzar vulnerabilitats en una organització
- No hi ha estàndards universals
- La metodologia depèn de què s'acorda amb el client
- Les companyies acostumen a tenir una metodologia de avaluació estàndard
- El treball ha de ser pactat amb antelació.

Una diferenciació interessant la fa Kevin G. Coleman en un article a TMCnet.com, a on defensa que una avaluació comprova l'estat de la implementació de mesures i programes de seguretat que existeixen en un conjunt de criteris (per exemple aquells que recull la ISO 27000), i que una auditoria és un registre formal de l'estat de seguretat actual de la companyia. Posa com a exemple un control d'accés: una avaluació comprovaria que la companyia té una política de contrasenyes fortes, mentre que una auditoria provaria de donar d'alta un usuari amb una contrasenya dèbil per comprovar que els controls estan implementats i funcionen. Les medicions que és fan en una auditoria son independents, motiu pel qual generalment l'auditor sempre és una persona externa a la companyia, mentre que les avaluacions sovint s'utilitzen per part de membres del personal.

2.1.2 Estratègies

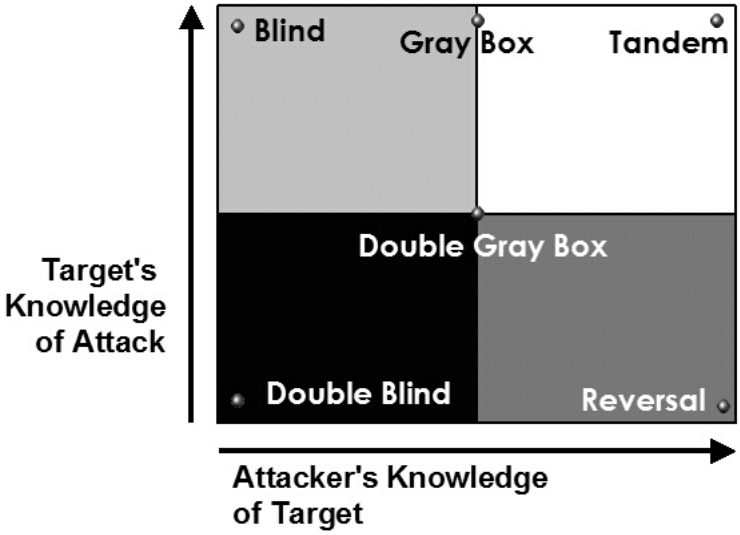

Fig. 2.1 Estratègies d'auditoria en funció del coneixement d'auditor i auditat

Es defineixen diferents estratègies d'auditoria en funció del coneixement que auditat i auditor tenen de l'altre. Les diferents estratègies són, entre d'altres, d'un dels següents sis tipus següents:

2.1.2.1 Cega

L'auditor encara l'objectiu sense coneixement previ de les seves defenses, actius, o canals. L'objectiu està preparat per l'auditoria, coneixent amb antelació tots els seus detalls. Una auditoria cega comprova principalment les habilitats de l'auditor. L'amplitud i profunditat de la auditoria venen determinades pels coneixements i eficiència aplicades de l'auditor. Aquesta estratègia sovint s'anomena Hacking ètic, War Gaming o Role Playing.

2.1.2.2 Doble cega

L'auditor encara l'objectiu sense coneixement previ de les seves defenses, actius, o canals. L'objectiu desconeix l'àmbit de l'auditoria, els canals comprovats, o els vectors de prova. Una auditoria doble cega comprova les habilitats del auditor i la preparació de l'objectiu davant variables desconegudes de pertorbació. L'amplitud i profunditat de la auditoria venen determinades pels coneixements i eficiència de l'auditor. També es coneguda com a auditoria de caixa negra, i és la estratègia emprada pel test de penetració.

Un test de penetració (*penetration testing* o *pen-test*) és una operació encoberta, en la que un expert en seguretat prova una sèrie d'atacs per a

esbrinar si un sistema pot suportar el mateix tipus d'atacs d'un *hacker* maliciós. Aquests atacs de prova poden incloure tot el que un atacant real pot provar, com la enginyeria social.

Sobre aquesta estratègia, Ira Winkler diu:

"W*hen you're being asked to evaluate the state of someone's system security, penetration tests are only marginally useful. Sure, they serve a purpose, but they are not the "silver bullet" some people perceive them to be*."

2.1.2.3 Caixa grisa

L'auditor encara l'objectiu amb coneixement limitat de les seves defenses i actius i ple coneixement dels canals. L'objectiu està preparat per l'auditoria, coneixent amb antelació tots els detalls de la auditoria. Una auditoria de caixa grisa comprova les habilitats del auditor i la preparació del objectiu davant variables desconegudes de pertorbació. La naturalesa d'aquest test és la eficiència. La amplitud i profunditat depèn de la qualitat de la informació proporcionada al auditor abans del test així com els coneixements de l'auditor. Aquest tipus de test sovint s'anomena test de vulnerabilitats i principalment s'utilitza com un mètode de autoavaluació per part de l'objectiu.

Una avaluació de vulnerabilitats consisteix en un estudi exhaustiu d'un sistema, cercant potencials punts dèbils. Sovint es realitza un escaneig del objecte, pel que també es coneix com a escaneig de vulnerabilitats.

L'objectiu coneix tots els detalls de l'auditoria, però no pot saber tot el que farà l'auditor ja que aquest tampoc ho sap. Per això aquest test també comprova la preparació del objectiu davant variables desconegudes.

2.1.2.4 Doble caixa grisa

L'auditor encara l'objectiu amb coneixement limitat de les seves defenses i actius i ple coneixement dels canals. L'objectiu ha estat notificat amb antelació del àmbit i finestra de temps de l'auditoria però no dels canals ni els vectors de prova. Una auditoria de doble caixa grisa comprova les habilitats de l'auditor i la preparació de l'objectiu davant variables desconegudes de pertorbació. La naturalesa del test és la eficiència. La amplitud i profunditat depèn de la qualitat de la informació proporcionada al auditor i l'objectiu abans del test així com els coneixements de l'auditor. Aquesta estratègia també s'anomena caixa blanca.

2.1.2.5 Tàndem

L'auditor i l'objectiu estan preparats per l'auditoria, ambdós coneixent amb antelació tots els detalls de l'auditoria. Una auditoria de tàndem comprova la protecció i els controls de l'objectiu. Tot i així, no pot comprovar la preparació d'aquest davant variables desconegudes de pertorbació. La naturalesa

verdadera d'aquest test és el rigor donat que l'auditor té visió plena de tots els test i de les seves respostes. La amplitud i profunditat depèn de la qualitat de la informació proporcionada al auditor abans del test (transparència) així com els coneixements de l'auditor. Aquest test és sovint conegut com una auditoria interna o de caixa de cristall, i l'auditor és sovint part del procés de seguretat.

2.1.2.6 Inversa

L'auditor encara l'objectiu amb ple coneixement dels seus processos i seguretat operacional, i l'objectiu desconeix què, com, o quan l'auditor comprovarà. La verdadera naturalesa d'aquest test és auditar la preparació del objectiu davant de variables desconegudes i vectors de pertorbació. La amplitud i profunditat depèn de la qualitat de la informació proporcionada al auditor i del seus coneixements i creativitat. Sovint també s'anomena exercici d'equip vermell (*Red Team*).

2.2 Tecnologia i estàndards WiFi

En aquest capítol, estudiarem la tecnologia WiFi per a situar les bases que ens permetran aprofundir en la seva seguretat operativa.

2.2.1 Context

Segons conclusions del "*II barómetro de la movilidad Dell – IDC*", WiFi és la tecnologia preferida majoritàriament (72%) per les empreses per a resoldre les seves necessitats de mobilitat dintre de la oficina.

Segons es desprèn de l'informe WiFi 2008 de Gowex, els usuaris de WiFi a Espanya:

- Creixen en número al ritme que ho feien els usuaris totals d'Internet en l'any 2004
- Seguint aquesta constant, superaran la xifra de 25 milions a l'any 2014
- Creixen quantitativament més ràpid que el global d'usuaris d'Internet

Com es veu en el següent gràfic de l'anterior informe, més de la meitat dels usuaris d'Internet a Espanya es connecten a través de WiFi (un 50,3 % de les llars espanyoles segons els darrer "*Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas*" de Juny de 2008).

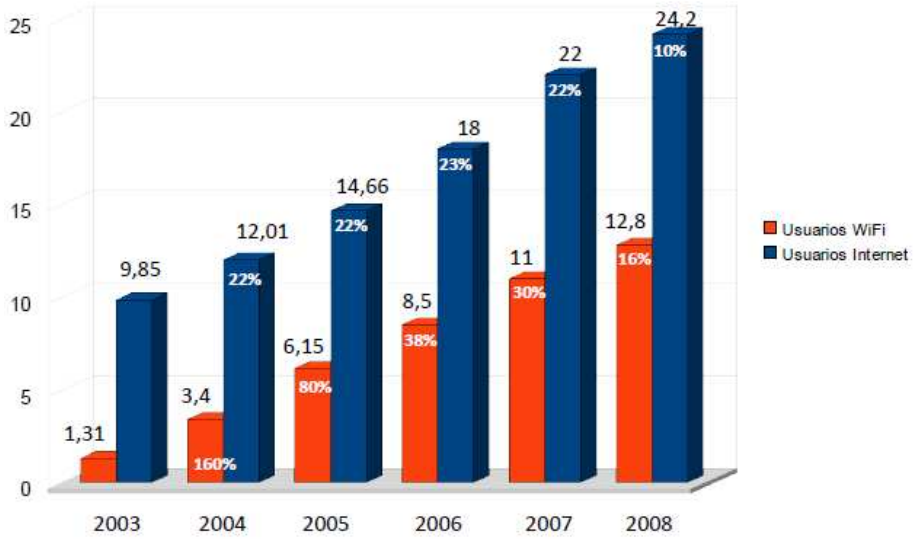

Fig. 2.2 usuaris WiFi i Internet (milions)

Gowex estima que en el 2014 el número d'usuaris potencials de WiFi superarà els 22 milions.

Segons l'INTECO, el *Instituto Nacional de Tecnologías de la Comunicación*, al voltant d'un 10 % d'usuaris WiFi domèstics han detectat un robatori de l'ample de banda d'Internet. Si ve aquesta dada és menor a les pimes (1,6%), aquests percentatges ens posen de manifest la manca de seguretat de les xarxes WiFi que són presents avui dia. Donat que WiFi es una tecnologia de connexió molt comuna, que sigui insegura ens introdueix un problema que va més enllà de les xarxes que administrem, i que també afecta a la mobilitat dels usuaris quan fan ús d'aquesta tecnologia, especialment si ho fan per accedir a la nostra xarxa. Les empreses no tenen prou en considerar la seguretat de les xarxes que posseeixen, sinó que s'ha de considerar també la protecció dels usuaris quan es connecten a d'altres xarxes WiFi.

La tecnologia WiFi ha tingut una rapidíssima propagació, i compta actualment amb milions d'usuaris en tot el món i és molt present a l'entorn empresarial. Aquesta difusió ha provocat que a pesar de la continua evolució de la seguretat WiFi, un gran nombre de les xarxes WiFi existents siguin insegures en diferents graus, ja que la tecnologia no oferia uns bons nivells de seguretat en els seus inicis.

Un dels motius de la ràpida acceptació de WiFi en entorns LAN és la seva capacitat de aprovisionar connectivitat en aquells entorns on la instal·lació de cablejat era impossible o molt costosa. En contrapartida, i degut a la seva naturalesa radio, WiFi és susceptible a una sèrie d'atacs nous, ja que en les comunicacions sense fils el medi físic és compartit, exposant les capes física i MAC a ser atacades a través de l'aire. Això obre una nova àrea als consultors de seguretat en auditar xarxes sense fils. Es fa necessària la implementació de

sistemes que assegurin la seguretat en les capes inferiors, ja que nous atacs, sovint propis de capes superiors, com la denegació de servei i la suplantació d'identitat, per citar-ne uns exemples, són ara possibles en aquestes.

De totes les tecnologies de connectivitat sense fils, aquests tipus d'atacs son especialment presents en les que ofereixen major rang de transmissió perquè això augmenta la possibilitat d'obtenir una bona ubicació física per a l'atac. D'altra banda, aquestes tecnologies WAN sense fils com GSM, GPRS o 3G utilitzen comunicació punt a punt (pel que certs tipus d'atacs són impracticables) i requeririen d'una infraestructura més cara, voluminosa i complexa per a realitzar els atacs. WiMAX (IEEE 802.16) és la tecnologia MAN sense fils emergent més similar a WiFi. En el seu disseny s'ha considerat la seguretat molt més profundament que en WiFi, tot i que molts atacs segueixen essent possibles. Però la tecnologia sense fils dominant en l'escala LAN es WiFi, per damunt d'alternatives com HiperLAN. El seu rang fa possible atacs des d'una ubicació física apropiada, alhora que la fa present en tots aquells entorns LAN que vulguin incorporar tecnologies sense fils. Tot i que tecnologies PAN sense fils com Bluetooth també són molt comunes, la seva cobertura i ús (difícilment s'utilitzen per a configurar una xarxa) col·loca a aquestes en un nivell de risc i dany potencial menor.

Taula 2.1 Tecnologies de xarxa sense fils

	PAN	LAN	MAN	WAN
Estàndards	Bluetooth, UWB, ZigBee	802.11 HiperLAN2	802.16 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G, 802.16
Velocitat	< 1Mbps	11 a 54 Mbps	11 a 100+ Mbps	10 a 384 Kbps
Rang	Curt	Mitjà	Mitjà – Llarg	Llarg
Aplicacions	P2P, Dispositiu a Dispositiu, Pico Net	Xarxes domèstiques i empresarials	Reemplaçament T1, accés d'última milla	PDAs, Telèfons mòbils

2.2.2 WiFi i WLAN

Donada la existent confusió entre els dos termes, es apropiada la inclusió d'un apartat a on s'aclareixin els termes tal i com es fan servir en aquest treball.

Des del 1997, el grup de treball 11 del comitè d'estàndards LAN/MAN del IEEE (IEEE 802 LMSC) ha publicat els estàndards de les xarxes sense fils d'àrea local (WLAN), de manera similar a com es va fer el seu dia amb altres estàndards:

802.1 Higher Layer LAN Protocols Working Group

802.2 Logical Link Control Working Group
802.3 Ethernet Working Group
802.4 Token Bus Working Group
802.5 Token Ring Working Group
802.6 Metropolitan Area Network Working Group
802.7 Broadband TAG
802.8 Fiber Optic TAG
802.9 Integrated Services LAN Working Group
802.10 Security Working Group
802.11 Wireless LAN Working Group
802.12 Demand Priority Working Group
802.14 Cable Modem Working Group
802.15 Wireless Personal Area Network (WPAN) Working Group
802.16 Broadband Wireless Access Working Group
802.17 Resilient Packet Ring Working Group
802.18 Radio Regulatory TAG
802.19 Coexistence TAG
802.20 Mobile Broadband Wireless Access (MBWA) Working Group
802.21 Media Independent Handoff Working Group
802.22 Wireless Regional Area Networks

Com es pot comprovar, existeixen diferents grups de treball per a diferents tecnologies LAN. D'aquesta manera, Ethernet, Token Bus i Token Ring, tecnologies concretes, tenen un grup de treball propi. No passa el mateix amb les xarxes WPAN, WLAN, MAN i WMAN, on el grup de treball no treballa en una tecnologia que disposi d'un nom comercial que representi una implementació concreta, tot i que aquestes existeixen: Bluetooth en 802.15.1, ZigBee en 802.15.4 i WiMAX en 802.16. La relació entre aquests noms i el estàndard relacionat varia en cada cas. En el cas de Bluetooth, el grup de treball 802.15.1 ha derivat el seu estàndard a partir de les especificacions de la Bluetooth v1.1 Foundation.

ZigBee, WiMAX i WiFi representen un cas al inrevés, en els que una organització sense ànim de lucre ha desenvolupat i certifica una implementació del estàndard i en posa un nom comercial.

Aquestes diferents relacions entre estàndard i tecnologia han provocat una enorme confusió. En les LAN, possiblement a causa d'existir més d'una tecnologia, l'IEEE ha treballat amb una especificació concreta amb un nom determinat: Ethernet, Token Bus i Token Ring. Però no està fent el mateix amb les WPAN, WLAN i WPAN. Qui ha implementat la tecnologia en aquest casos és una altre entitat. Degut a que un acrònim com WLAN, que hauria de agrupar les xarxes sense fils d'àrea local, s'utilitza per part de l'IEEE per fer referència als estàndards que publica d'una tecnologia en concret (podrien haver-n'hi d'altres dintre de la categoria de la mateixa manera com n'hi ha diverses a LAN) el terme s'ha trencat i ha perdut tot el seu sentit classificador original.

A la pràctica, això ha causat que WLAN es prengui de vegades com una implementació de la tecnologia (WiFi) i d'altres per a classificar erròniament xarxes, però perdent tot el sentit original i utilitzant-se com a un denominador

per a fer referència a totes les xarxes sense fils independentment de la seva mida. Molt poques vegades s'utilitza correctament. I és que WLAN, entès com a un tipus de xarxa, nomes té un estàndard i una implementació a la pràctica, WiFi.

Es molt habitual trobar a Internet pàgines que parlen de tecnologies WLAN englobant-hi Bluetooth, WiMAX, ZigBee, i demés. I també és molt habitual trobar extensos articles d'opinió en els que es parla de com altres tecnologies son superiors a WLAN en una comparativa sense sentit.

Una mostra de com l'estàndard WLAN està escrit com una norma que cal implementar la trobem al mateix estàndard:

"IEEE Std 802.11 logically separates the WM from the distribution system medium (DSM). Each logical medium is used for different purposes, by a different component of the architecture. The IEEE 802.11 definitions neither preclude, nor demand, that the multiple media be either the same or different. Recognizing that the multiple media are logically different is key to understanding the flexibility of the architecture. The IEEE 802.11 LAN architecture is specified independently of the physical characteristics of any specific implementation."

En aquest treball els dos termes poden aparèixer utilitzats indistintament, sempre que el context ho permeti, tenint en compte el seu significat tal i com s'ha explicat aquí, és a dir, sempre que el què s'estigui tractant sigui comú a l'estàndard i a la seva implementació.

2.2.3 Arquitectura IEEE 802.11

La arquitectura 802.11 consisteix en diferents components que interactuen per a proveir una WLAN que suporti una mobilitat transparent de la STA (*station*) a les capes superiors.

El BSS (*Basic Service Set*) és el bloc basic d'una LAN IEEE 802.11. Està constituït per diverses STA dintre d'una area de cobertura (BSA). Pot ser independent (IBSS), formant el que s'anomena una xarxa ad hoc, sent aquest el tipus mes bàsic de xarxa IEEE 802.11, o pot ser un component d'una infraestructura major, de mida i complexitat arbitraries, anomenada ESS (*Extended Service Set*).

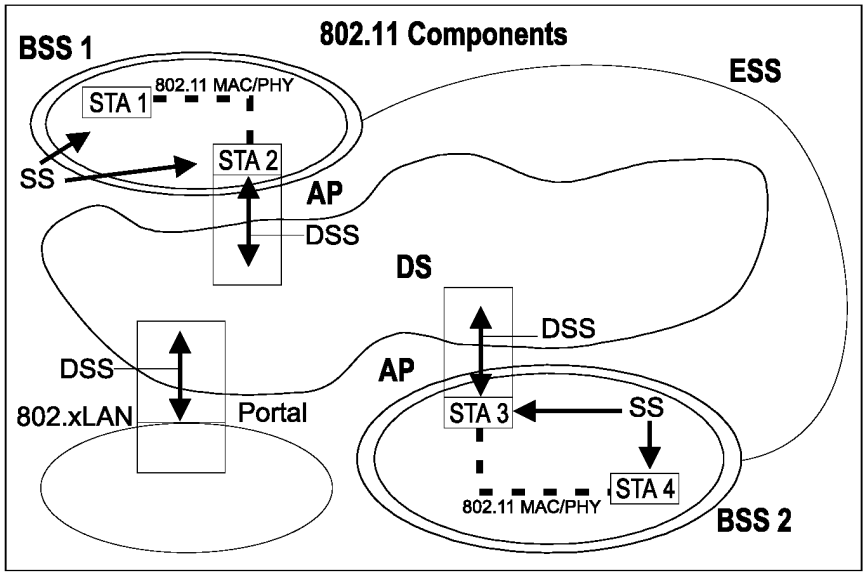

Fig. 2.3 Components de la arquitectura IEEE 802.11

Una ESS és la unió de diversos BSS connectats a través d'un DS (*Distribution Service*), però que no inclou aquest. Les dades es mouen entre un BSS i un DS a través d'un AP (*Access Point*), dispositiu que és també una STA, i que per tant és adreçable. Les adreces utilitzades per a la comunicació del AP en el medi sense fils i el medi del DS no han de ser necessàriament les mateixes.

El concepte clau és que la xarxa ESS aparegui de la mateixa manera a la capa LLC com una xarxa IBSS. Les STA dintre un ESS poden comunicar-se i aquelles que siguin mòbils poden moure's d'un BSS a un altre dintre del mateix ESS de manera transparent a l'LLC.

Una o més IBSS o ESS poden ser presents en el mateix espai que d'altres. Això pot donar-se per una sèrie de raons. Alguns exemples son quan una xarxa ad hoc opera en una ubicació en la que ja es troba una ESS, quan dues xarxes desplegades per diferents organitzacions es superposen parcialment, o quan dos o més accessos o politiques de seguretat son necessàries en el mateix espai. Físicament, es poden donar els següents casos:

a) Superposició parcial. Habitualment s'utilitza per a proporcionar cobertura continua a l'espai.
b) No superposició. No hi ha límit de distancia entre BSS.
c) Superposició total. Pot utilitzar-se per a proporcionar redundància.

2.2.4 Consideracions de seguretat de la arquitectura

La capa física utilitzada en l'estàndard 802.11 del IEEE és fonamentalment diferent del medi cable. En conseqüència, aquesta capa:

a) Utilitza un medi que no té fronteres observables.
b) Està desprotegida davant altres senyals que poden estar compartint el medi.
c) Té topologies dinàmiques.
d) Manca de connectivitat total, així que la habitual assumpció de que totes les STA poden escoltar a totes les altres STA és invàlida, i per tant, poden haver-hi STA ocultes d'altres.
e) Pot experimentar interferències provinents d'altres xarxes 802.11 separades lògicament que operin en una àrea solapada.

Aquestes característiques són el punt de partida per l'estudi de la seguretat WiFi a continuació.

2.2.5 Comunicacions WiFi segures

Les característiques que defineixen la seguretat informàtica són les següents:

Integritat: La informació només pot ésser modificada per qui està autoritzat i de manera controlada
Confidencialitat: La informació només ha de ser llegible pels autoritzats.
Disponibilitat: La informació només ha d'estar disponible quan es necessita.
Irrefutabilitat (No repudi): L'ús i/o modificació de la informació per part d'un usuari ha de ser irrefutable.

En el cas de la seguretat en WiFi, aquesta tracta fonamentalment de **controlar l'accés** i **garantir la privacitat.** Si bé els mecanismes que intenten garantir la no intrusió de persones o *software* no autoritzat a la xarxa proveeixen d'integritat i confidencialitat, els altres dos aspectes que defineixen la seguretat clàssica no queden especialment coberts.

Una definició que resumeix bé tot això la recull la *Wikipèdia* sota el terme *Wireless security*, que tot i que vindria a traduir-se com a seguretat a les tecnologies sense fils, fa referència a la seguretat en 802.11:

"Wireless security is the prevention of unauthorized access or damage to computers using wireless networks".

En aquest capítol s'examinen les diferents tècniques, tecnologies, protocols i sistemes per tal de aconseguir que una xarxa WiFi esdevingui segura.

2.2.6 Història de la seguretat de WiFi a través de dues aproximacions de seguretat

Tenint en compte les consideracions anteriors, en aquest apartat estudiarem el tractament aplicat a les WLAN per obtenir seguretat a través de dues aproximacions.

A tal efecte, definirem una arquitectura bàsica de seguretat ja existent en la que integrar la WLAN:

Fig. 2.4 Arquitectura bàsica de seguretat

2.2.6.1 1a opció: Col·locar la WLAN en la zona insegura

Per tal de combatre la consideració 'a' exposada anteriorment a l'apartat 2.2.4, es fa necessari que tots els usuaris de WLAN passin a la zona insegura, ja que aquesta xarxa no pot ser continguda físicament (i.e. la cobertura WLAN pot estendre's a fora de l'edifici o a zones considerades no segures), independentment de la ubicació real del usuari.

Fig. 2.5 Introducció de WLAN en la arquitectura

Un abordatge a aquesta situació consisteix en gestionar els usuaris WLAN de la mateixa manera que es gestionen els usuaris remots. La tecnologia VPN proporciona una manera d'estendre la zona segura a usuaris situats en la zona insegura (per exemple, aquells que es connecten des d'ubicacions remotes).

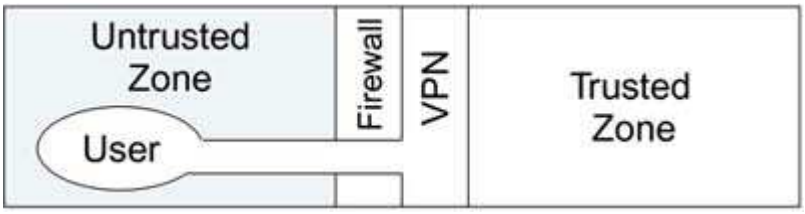

Figura 2.6 Incorporació de VPN a la arquitectura

Utilitzant VPN per a connectar-se a la zona segura, els usuaris WLAN poden tornar a ingressar a la zona segura.

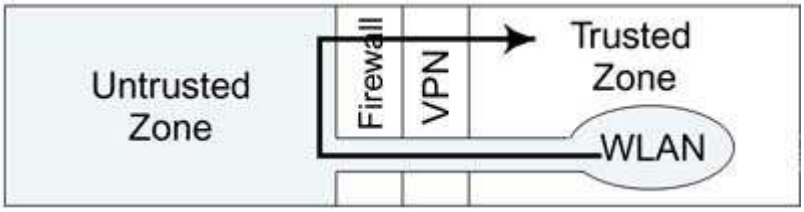

Fig. 2.7 WLAN a través de VPN

Aquesta aproximació presenta diferents desavantatges

- El software VPN pot ser intrusiu, alentint les comunicacions i limitant el tipus d'operacions que es poden realitzar.
- El servidor VPN s'ha de dimensionar en funció del número de usuaris WLAN.
- Els punts d'accés no poden connectar-se a la LAN. Necessiten una estructura de cablejat dedicat que es connecti al tallafocs.

Aquests inconvenients fan que aquesta aproximació no sigui atractiva per moltes companyies així com impracticable per l'entorn domèstic i de la petita oficina. Moltes companyies han utilitzat aquesta aproximació durant les primeres generacions de WiFi per a combatre la manca de seguretat.

Així mateix, aquests inconvenients també fan que la majoria d'entorns prefereixen la següent aproximació, en la que WiFi esdevé part de la zona segura, tot i que la implementació d'aquesta primera aproximació s'utilitza sovint com a mesura de proporcionar una seguretat addicional o redundant.

2.2.6.2 2a opció: Col·locar la WLAN en la zona segura

En un principi, col·locar la WLAN dintre de la zona segura passava per aconseguir que la pròpia xarxa WLAN fos el més impenetrable possible en el nivell físic, de manera similar a tal i com ho és la xarxa per cable. En aquestes

línies de pensament el IEEE 802.11 va desenvolupar WEP (*Wired Equivalent Privacy*). En una primera instància, l'objectiu va ser dotar a WLAN d'una resistència davant a atacs major que la xarxa per cable, de tal manera que per un atacant fos més fàcil atacar aquesta. Aquest principi va quedat desfasat, i quan WEP va ser compromès al 2001, el IEEE va establir un grup (802.11i) dedicat a trobar un substitut, més centrat en les seves qualitats absolutes que en les relatives als atacs en un entorn on coexistia amb xarxa per cable.

Mentre el 802.11i treballava, la *WiFi Alliance* va presentar *WiFi Protected Access* (WPA) al 2003 com una solució de seguretat provisional per a tractar la demanda del mercat per a mecanismes de seguretat mes robustos mentre la correcció del IEEE es desenvolupava. WPA utilitza TKIP (*Temporal Key Integrity Protocol)*, conegut originalment com WEP2, que permetia als usuaris de WEP fer un *upgrade* del *sotfware* sense invertir en nou *hardware*. Els productes WPA van veure la llum a mitjans del 2003.

El treball del 802.11i va donar els seus fruits al Juny del 2004 i va ser implementat per la *WiFi alliance* com a WPA2. Utilitza CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code*) elaborat a partir d'AES en compte del RC4 de TKIP i WEP.

Actualment, el xifrat recomanat per l'entorn domèstic i de la petita oficina és WPA2-PSK (*Pre-Shared Key*, clau precompartida), tot i que l'ús de PSK a WPA o WPA2 presenta vulnerabilitats que condicionen les característiques de les claus com veurem més endavant. En l'entorn empresarial, és WPA2 amb EAP-TLS conjuntament amb un servidor RADIUS.

Un cop la informació enviada a través de WiFi és completament inaccessible als atacants (potser més que la que circula per un cable), l'equipament WiFi pot ser tractat de la mateixa manera que els dispositius LAN. Els punts d'accés poden utilitzar la LAN com a DS (*Distribution Service*), reduint així la infraestructura necessària.

3. CAPÍTOL 3. SEGURETAT WIFI

Ja assentades les bases del treball, aquest capítol aprofundeix en la seguretat de la tecnologia 802.11, per tal d'obtenir un nivell de coneixements apropiat per la millora del servei d'una xarxa WiFi.

3.1 Vulnerabilitats de 802.11

En aquest apartat s'analitzen les vulnerabilitats pròpies del protocol 802.11 i dels mecanismes i tècniques utilitzats per a la seguretat de la tecnologia.

Degut a que el primer estàndard 802.11 incorporava com a part integrant WEP com a únic xifrat, i que les principals vulnerabilitats que han fet que aquest xifrat hagi estat trencat tenen a veure en la interacció de 802.11 amb el xifrat, no resulta fàcil una classificació separada per aquest últim. D'aquesta manera, les vulnerabilitats 2.2.4 i 2.2.5 que aquí es recullen han nascut en aquesta interacció, i no es troben dintre de les vulnerabilitats pròpies del xifrat, tot i que els atacs conseqüents només escometen contra WEP.

3.1.1 Vulnerabilitats d'identitat

Les vulnerabilitats d'identitat sorgeixen de la confiança explicita que 802.11 té en la adreça origen d'un paquet rebut. Per a les trames de gestió, 802.11 no inclou cap mecanisme que permeti verificar la veracitat de la identitat informada. En conseqüència, un atacant pot suplantar un altre node i realitzar peticions de servei en el seu nom.

3.1.2 Vulnerabilitats en la autenticació

L'estàndard 802.11 defineix dues formes d'autenticació: *Open System* (sense autenticació) i *Shared Key* (clau compartida).

Tot i que la idea original de la segona era que seria millor que la no autenticació perquè l'usuari havia de demostrar el coneixement de la clau WEP (l'estàndard original nomes contemplava WEP com a mecanisme de xifrat), en realitat aquest sistema redueix la seguretat de la xarxa i fa fàcil la recuperació de la clau WEP. Aquest sistema utilitza el xifrat d'un desafiament. Donat que un atacant pot observar el desafiament i la resposta, pot determinar el *keystream* utilitzat per al xifrat, podent-lo utilitzar per a autenticar-se. Una altre flaquesa del sistema radica en que aquest permet a un client conèixer ràpidament la validesa d'una clau WEP, el que permet atacs per diccionari. El sistema també ofereix avantatges, com la reducció dels efectes d'un atac DoS amb paquets

xifrats amb una WEP incorrecta, però els inconvenients representen uns riscos de seguretat tan elevats que és més segura la utilització de la autenticació *Open System*. Si es vol aconseguir una bona autenticació, s'hauran d'implementar altres protocols, com 802.1x.

3.1.3 Vulnerabilitats en les tècniques de control d'accés

Les dues tècniques següents són tècniques primitives que van sorgir mentre els mecanismes de xifrat van desenvolupar-se i estendre. Així mateix, als inicis de l'aparició de WEP, les regulacions dels EE.UU. no permetien la exportació de productes criptogràfics de més 40 bits i, a més, la potència necessària en aquell moment per a la capa MAC del 802.11 era tal que molts fabricants van buscar alternatives per al control d'accés en tècniques que estan fora de l'estàndard.

3.1.3.1 Filtrat MAC

Una de les tècniques més senzilles és configurar el punt d'accés per permetre la connexió només a adreces MAC conegudes. Aquestes adreces poden ser suplantades, però l'esforç que ha de dedicar un atacant per obtenir accés a la xarxa és major i pot ser descobert amb més facilitat en negar el servei a la estació de qui pren la adreça.

3.1.3.2 Ocultació del ESSID

Un altra tècnica molt senzilla i àmpliament implementada als punts d'accés és la possibilitat d'ocultar el ESSID, que té com a objectiu fer invisible la xarxa al descobriment i a la associació de clients no autoritzats. El AP mostra un SSID null a les trames beacon i no respon a trames *probe request* que no continguin el SSID corresponent ("ANY" o "NULL"). Quan el SSID és coincident, el AP pot respondre en alguns casos amb un SSID null, evitant la recuperació del SSID amb un atac de desassociació. Els beacons han de seguir emetent-se per a poder gestionar, entre d'altres, l'estalvi d'energia i per a que els clients segueixin actius (en Windows XP SP2) i, d'aquesta manera, només les estacions que coneguin la existència de la xarxa i el seu ESSID podran connectar-se. Tot i així, un sniffer passiu és capaç de detectar aquest tipus de xarxes. Aquesta tècnica és coneguda com a *closed mode, closed network mode, cloacked mode, stealth mode, private network, SSID broadcasting*,... en funció del fabricant.

3.1.4 Vulnerabilitat de text conegut

La porció inicial dels paquets 802.11 és pràcticament constant. Un paquet comença amb una capçalera LLC seguida per una SNAP. Aquestes dues capçaleres ocupen els 8 primers bytes del paquet. L'únic camp desconegut és

el *ethertype* del final de la capçalera SNAP. Habitualment, aquest serà ARP o IP.

Els paquets ARP són fàcilment distingibles per la seva longitud de 36 bytes i són habitualment dirigits a adreces *broadcast*. Algun *hardware* farceix els paquets curts a una llargada mínima, fent els paquets ARP més llargs. Inspeccionant el prefix MAC del AP, es pot determinar el hardware en ús i esbrinar si això es produeix o no. Podent diferenciar els paquets IP dels ARP, coneixem els primers 8 bytes del text en clar de cada paquet.

A partir d'aquí, 8 bytes del *keystream* WEP poden ser calculats a partir del XOR del text clar amb el xifrat, que ens permetran xifrar un *payload* (informació útil de cara a la capa inferior) de 8 bytes, composat per 4 bytes de dades y 4 del seu corresponent CRC32.

Degut a que la capçalera LLC/SNAP té una mida de 8 bytes, aquesta vulnerabilitat mai es va considerar problemàtica, fins que va ser aplicada conjuntament amb la següent.

3.1.5 Vulnerabilitat en la fragmentació

L'estàndard 802.11 especifica la fragmentació a la capa MAC. És possible l'enviament de múltiples fragments (fins a 16) utilitzant el mateix *keystream* WEP.
Explotant la vulnerabilitat de text conegut que permet l'obtenció de fins a 8 bytes de *keystream*, l'enviament de *payloads* en fragments de 8 bytes fa possible injectar 64 bytes de dades.

3.1.6 Vulnerabilitats del xifrat WEP

La primera solució del IEEE (1997, ratificada el setembre de 1999 en la secció 8.2 del estàndard) davant de les necessitats de seguretat va ser WEP (*Wired Equivalent Privacy*). Les seves característiques són:

- Xifra tots els paquets enviats mitjançant l'algoritme de xifrat RC4 per a la **confidencialitat**, amb una única clau compartida entre tots els dispositius
- Utilitza una suma de verificació CRC-32 que proporciona la **integritat** per a prevenir la reinjecció de paquets modificats.

Cada paquet es xifra separadament fent una operació XOR amb un *keystream* (seqüència de nombres pseudoaleatoris) RC4 generat per una llavor de 64 o 128 bits, composada per la concatenació d'un vector d'inicialització (IV) de 24 bits i una clau WEP de 40 (segons l'estàndard) o 104 bits (segons la implementació de la indústria anomenada WEP2 o WEP-128).

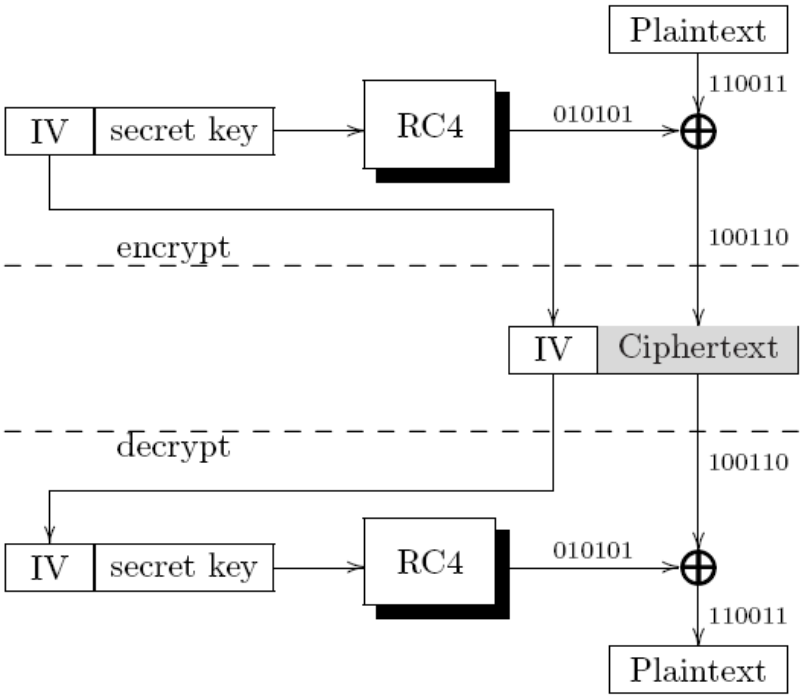

Fig. 3.1 Esquema de xifrat WEP

Un número pseudoaleatori és generat en un procés que sembla produir nombres al atzar, però no ho fa realment. Tot i que les seqüències de números pseudoaleatoris no mostren cap patró o regularitat aparent des d'un punt de vista estadístic, han estat generades per un algorisme completament determinista en el que les mateixes condicions inicials produeixen sempre el mateix resultat. A causa d'això, es necessita un Vector d'Inicialització (IV) que ha de ser escollit per l'emissor i que ha de ser canviat de tal manera que cada paquet es xifri amb *keystream* diferent, i que s'envia en clar per que el receptor pugui desxifrar el missatge.

Un *Integrity Check Value* (ICV) de 4 bytes és calculat del paquet original mitjançant el algorisme de comprovació CRC-32 i annexat al final. L'ICV també es xifra amb el *keystream* RC4.

Tot seguit es recullen les principals vulnerabilitats conegudes:

3.1.6.1 Gestió i mida de la clau:

La gestió de la clau no està especificada en l'estàndard WEP, i com a conseqüència és una de les seves debilitats, perquè sense una gestió interoperable de claus, aquestes tendeixen a romandre massa temps i ser de baixa qualitat. Tenint en compte que la sincronització dels canvis de clau entre AP i STAs és tediosa,les claus són rarament canviades.

L'única mida de la clau que especifica l'estàndard de 40 bits, també és una debilitat del protocol. Quan l'estàndard va ser escrit al 1997, les claus d'aquesta longitud eren considerades raonables per a algunes aplicacions. Donat que l'objectiu era protegir contra escoltes ocasionals, semblava suficient. Els EE.UU. no controlaven estrictament les exportacions de xifrats de fins a 40 bits, i l'IEEE va voler assegurar la exportació dels dispositius WiFi. Amb la potència de càlcul actual, es pot trobar la clau mitjançant un atac de força bruta en menys d'un mes utilitzant un sol ordinador.

La majoria dels fabricants van implementar un estàndard de facto, estenent senzillament la longitud de la clau fins als 104 bits, amb una excel·lent interoperabilitat. Sovint aquesta s'anomena clau WEP de 128 bits. Tot i que la mida de la clau és major (104 bits, 13 caràcters ASCII o 26 hexadecimals), es manté la mateixa mida del IV, 24 bits, provocant que tant en el WEP de 64 com el de 128 bits hi sigui present la vulnerabilitat següent:

3.1.6.2 Repeticions de IV:

L'estàndard 802.11 no especifica com gestionar el IV. Tot i que s'indica que ha de canviar-se en cada trama, això no és obligatori. Com a conseqüència, una bona part de les implementacions han optat per que l'IV sigui un comptador que comenci de zero, de tal manera que les primeres combinacions es repeteixen freqüentment en el medi, ja que cada estació utilitza la mateixa clau, i així mateix cada cop que el *hardware* s'inicia.

D'altres implementacions escullen el IV aleatòriament. D'aquesta manera, hi ha un 50% de possibilitats de repetició amb només 5000 IVs.

Tanmateix, el nombre d'IV possibles no és massa elevat (2^{24} = 16,777,216) pel que les repeticions succeeixen i augmenten amb la càrrega de la xarxa. Donat que l'IV s'envia en clar, és possible identificar les repeticions.

A partir d'aquí, diferents atacs son possibles donada la relació entre IV-*keystream* i que obtenir aquest és molt més senzill que obtenir la clau WEP. Com ja hem vist, el *keystream* que genera el *Pseudo-Random Generation Algorithm* (PRGA) del RC4 serà sempre igual donada una llavor determinada. Una vegada conegut, un atacant pot desxifrar i falsificar paquets amb el mateix IV sense conèixer la clau WEP (veure desxifratge a la figura 3.1).

3.1.6.3 El Integrity Check Value no és apropiat:

El ICV es calcula utilitzant CRC-32, un algoritme excel·lent per a la detecció de soroll, però una opció inadequada per a un *hash* criptogràfic, ja que és una funció lineal que permet que un atacant canviï el ICV d'un missatge que ha modificat.

3.1.6.4 El ús del RC4 no és apropiat: Debilitat del IV:

El 26 de Setembre de 1995 David Wagner de la universitat de Berkeley va publicar a *sci.crypt* una potencial vulnerabilitat del RC4.

El 27 d'Octubre de 2000 Jesse R. Walker de la Intel Corporation va redactar la primera publicació on s'analitzen conjuntament la debilitat del IV i el mal ús del RC4 que fa WEP, demostrant la inseguretat de WEP i proposant correccions severes.

El 2001, Scott Fluhrer, Itsik Mantin, i Adi Shamir (d'ara endavant FMS) publiquen el seu anàlisi del xifrat RC4, on demostren que la implementació del RC4 que fa WEP té claus dèbils. Aquestes claus guarden més relació amb la sortida que la adequada per a mantenir la seguretat. En l'ús que WEP fa del RC4, esbrinar quins paquets han estat xifrats amb una clau dèbil és fàcil perquè els tres primers paquets de la clau corresponen amb els de l'IV transmès en clar.

Aquest atac va ser millorat el 2004 per un *hacker* anomenat KoreK.

El 2005, Andreas Klein va presentar un nou anàlisi del xifrat RC4, trobant més correlacions entre *keystream* i clau.

3.1.7 Vulnerabilitats del xifrat WPA

TKIP va desenvolupar-se com una millora de WEP (utilitzava el mateix RC4) i va corregir-ne les vulnerabilitats proveint:

- Autenticació via RADIUS (basat en 802.1x) o via PSK.
- Claus dinàmiques, que conjuntament amb un IV més gran evita la vulnerabilitat 3.1.6.2.
- Millora l'IV (*Initialization Vector*) amb una longitud de 48 bits.
- Un xifrat més fort a través d'una clau més llarga de 128 bits.
- Claus per paquet.
- Incorpora un nou mecanisme de comprovació d'integritat anomenat MIC (*Message Integrity Code*, també conegut com Michael).
- Un comptador de trames que evita els atacs per repetició.

En WPA, una clau mestre (PMK, *Pairwise Master Key*) és compartida entre l'AP i els clients. Aquesta clau genera dos tipus de claus, la clau MIC de 64 bits i la clau de xifrat de 128 bits. El codi MIC es genera a partir de la clau MIC i dades.

3.1.7.1 Vulnerabilitats de PSK

Al 2003, Moskowitz analitzava les vulnerabilitats d'utilitzar autenticació PSK, destinada a entorns domèstics o de petita oficina on desplegar RADIUS era massa costós o complicat.

Una PSK és un número de 256 bits o una paraula clau de 8 a 63 bytes. Cada estació pot tenir la seva propia PSK, vinculada a la seva adreça MAC, però els fabricants només proveeixen una PSK per tot l'ESS, tal i com es feia amb WEP.

Quan una PSK s'utilitza en comptes de 802.1x, la PSK és la PMK utilitzada durant el *4-way handshake* i tota la jerarquia de claus PTK (*Pairwise Transient Key*, un conjunt temporal de claus operacionals – veure figura 3.2). La conversió d'un paraula clau PSK a un número de 256 és directa.

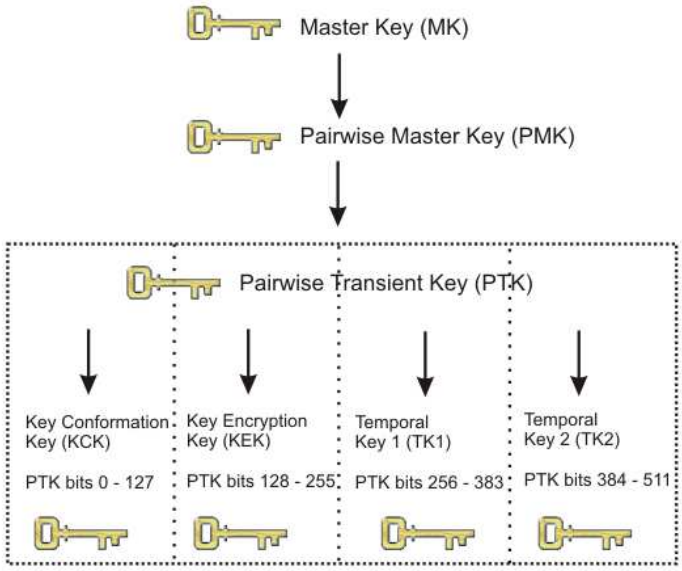

Fig. 3.2 Jerarquia de claus WPA

PTK es deriva de la PMK, MAC del AP, MAC del client i dos números aleatoris (ANonce i SNonce, dels dos primers paquets del *4-way handshake*). Té 512 bits i consta de diverses claus temporals dedicades:

1. KCK (Key Confirmation Key 128 bits): Clau per l'autenticació de missatges (MIC) durant el *4-Way Handshake* i el *Group Key Handshake.*
2. KEK (Key Encryption Key 128 bits): Clau per assegurar la confidencialitat de les dades durant el *4-Way Handshake* i el *Group Key Handshake.*
3. TK (Temporary Key 128 bits): Clau per encriptació de dades.
4. TMK (Temporary MIC Key – 2 de 64 bits): Clau per l'autenticació de dades (usada per MIC). S'utilitza una clau dedicada per cada costat de la comunicació.

Donat que cada emparellament unicast a l'ESS té claus PTK úniques, es garanteix la privacitat de les comunicacions entre AP i STA en WPA.

La vulnerabilitat recau en que tota la informació per derivar la PTK es pot obtenir amb la excepció de la PMK, pel que si aquesta es té (e.g. demés estacions emparellades) es poden desxifrar les comunicacions entre les altres STA i l'AP.

3.1.7.2 Vulnerabiilitat de MIC

El nou mecanisme d'integritat de WPA corregeix les vulnerabilitats del seu predecesor, però continua no sent una funció de *hash* pel que es invertible.

3.2 Atacs

3.2.1 Basats en suplantació d'identitat

Aquests atacs es basen en les vulnerabilitats d'identitat. Repetint els atacs de desautenticació o desassociació a clients es pot realitzar un atac DoS dirigit a una estació o a tot el canal. En aquest cas, el atac de desautenticació és més eficient que el de desassociació ja que porta la víctima a un estat inferior:

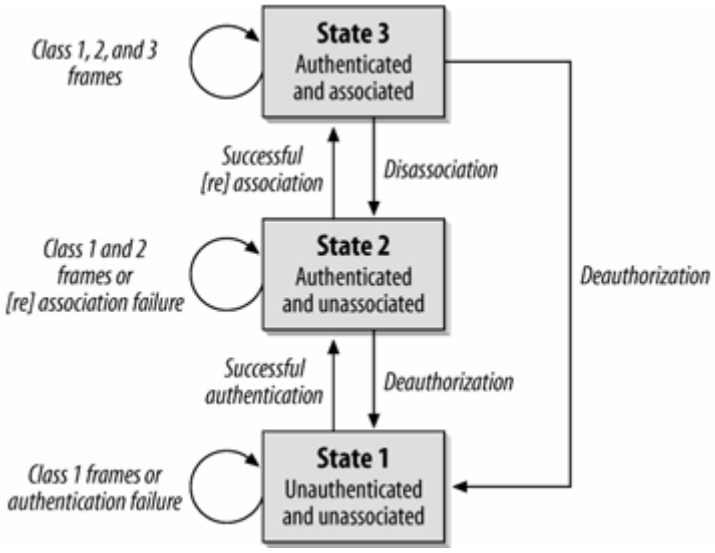

Fig. 3.3 Estats de 802.11

Aquest atac té l'avantatge que està dirigit als clients directament i l'AP o l'IDS poden no registrar-lo, especialment si queden fora de la cobertura del atacant.

3.2.1.1 Desautenticació

Un atacant pot enviar aquesta trama de gestió de classe 1 a un o tots els clients per a forçar una reautenticació.

3.2.1.2 Desassociació

Un atacant pot enviar aquesta trama de gestió de classe 2 a un o tots les STA per a forçar una reassociació. L'eina *Aircrack* anomena aquest atac *deauthentication*.

3.2.1.3 Estalvi d'energia

Per tal d'estalviar energia, les STA poden entrar en estat de suspensió durant el qual no poden comunicar-se. Abans d'entrar-hi, el client comunica la seva intenció per tal de que el AP comenci a emmagatzemar en memòria cau el tràfic destinat al node. De manera sincronitzada, la STA es desperta i demana pel tràfic pendent. Suplantant el node, un atacant pot aconseguir que un AP buidi el *buffer* de paquets destinats al la estació. Falsejant els missatges TIM (*Traffic Indication Map)* que indiquen la presència de paquets emmagatzemats es pot aconseguir el mateix efecte sense que el AP buidi el *buffer*. Modificant el període dels missatges TIM i el *timestamp* que el AP envia en *broadcast*, es pot trencar la sincronització necessària entre el AP i la STA en suspensió.

3.2.2 Trencament del xifrat WEP

A continuació es detallen tres tipus diferents d'atacs. Finalment s'anomenen els principals atacs coneguts.

3.2.2.1 Atacs per IV

Aquests es basen en atacar el subgrup de paquets amb el mateix IV, explotant les vulnerabilitats *Repeticions de IV* (3.1.6.2) i *Debilitat del IV* (3.1.6.4).

El principal avantatge dels atacs basats en IV o ICV és que són independents de la longitud de la clau.

Com ja hem vist, una vegada conegut el *keystream* per un paquet, un atacant pot desxifrar i injectar paquets amb el mateix IV (i per tant amb el mateix *keystream*) sense conèixer la clau WEP. Per obtenir-lo, podem fer el XOR del missatge xifrat amb el seu missatge en clar, que es pot preveure (Tràfic ICMP, ACK's TCP,….) o provocar (si la víctima té accés a Internet). Això ens permetria elaborar un diccionari amb les 16.777.215 possibilitats de IV que ens permetria desxifrar tot el tràfic.

Per altre banda, obtenir el XOR de dos paquets en clar és tan senzill com obtenir el XOR de dos paquets xifrats amb el mateix IV. Si coneixem o provoquem un missatge, l'altre és deduïble fent el XOR del primer per el XOR del xifrat d'ambdós.

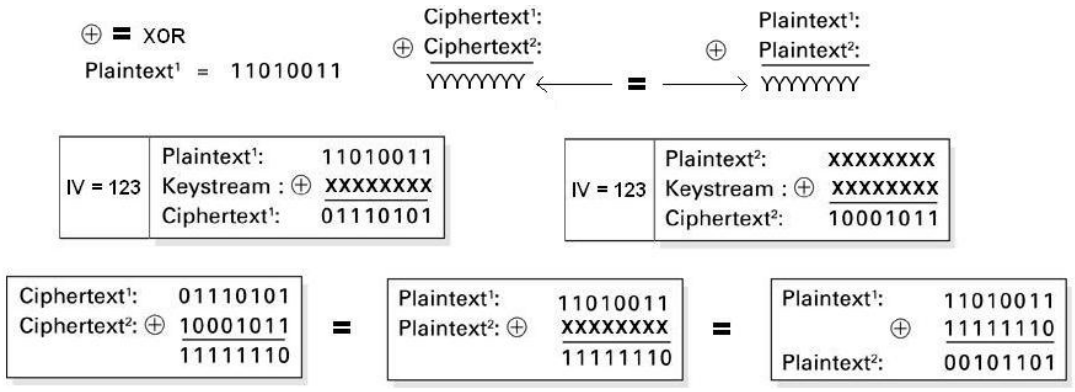

Fig. 3.4 Obtenció del text d'un missatge a partir d'un segon i del xifrat d'ambdós

3.2.2.2 Associació

En la autenticació de clau compartida, el AP transmet 128 bytes de text en clar, i la estació respon amb el text xifrat amb la mateixa clau i xifrat que utilitza WEP per a xifrar el subseqüent tràfic de xarxa. Aquests dos missatges poden ser interceptats molt fàcilment utilitzant un sniffer WiFi, d'on es pot calcular el *keystream*. Aquest *keystream* ens permetrà injectar paquets a la xarxa i autenticar-nos en el sistema d'autenticació de clau compartida. Aquest atac pot combinar-se amb d'altres com la desautenticació o desassociació de clients per a elaborar un diccionari que relacioni els IV amb el seu *Keystream*.

3.2.2.3 Atac de fragmentació

Aquest atac permet la injecció de paquets i, si la víctima està connectada a Internet, el desxifratge en temps real, que invalida el canvi periòdic de la clau WEP.

La injecció s'aconsegueix capturant un paquet i recuperant 8 bytes de *keystream*. Aquest es calcula a partir del text xifrat capturat i els 8 primers bytes que es coneixen del text en clar. A partir d'aquí, un atacant pot utilitzar la fragmentació 802.11 per injectar fins a 64 bytes de dades. Es pot utilitzar fragmentació IP per enviar paquets més llargs.

L'AP coneix la clau de xifrat, i pot ser utilitzat per al desxifrat del paquet capturat. Es pot utilitzar la fragmentació per afegir una capçalera IP a davant del paquet capturat, reenviar ambdós fragments,i així fer que el AP no l'enviï al seu destinatari legítim, sinó com un sol paquet en clar a una adreça que

controlem a través d'Internet. 802.11 no realitza cap comprovació per assegurar que un *payload* ja enviat no es reenviï com un fragment.

3.2.2.4 Cronologia de la mort de WEP

Aquesta és una petita cronologia dels principals atacs contra el xifrat WEP:

Maig 2001
Atac inductiu: "*An inductive chosen plaintext attack against WEP/WEP2*". William A. Arbaugh

Juliol 2001
Atac CRC bit flipping: "*Intercepting Mobile Communications: The Insecurity of 802.11*".
Borisov, Goldberg i Wagner.

Agost 2001
Debilitat del RC4: "*Weaknesses in the Key Scheduling Algorithm of RC4*".
Fluhrer, Mantin i Shamir".

Febrer 2002
Atacs FMS optimizats. h1kari

Agost 2004
Atacs IVs únics. KoreK

1 Abril 2007 (revisat el 16 de setembre del mateix any)
"*Breaking 104 bit WEP in less than 60 seconds*"
Erik Tews, Ralf-Philipp Weinmann and Andrei Pyshkin (d'ara endavant PTW)

Les estadístiques dels principals tipus d'atacs que s'utilitzen avui en dia són:

Atac FMS (2001):
Amb 4.000.000 a 6.000.000 IV, probabilitat d'èxit del 50%.

Atac KoreK (2004) per a 104 bits:
Amb 700.000 IV, probabilitat d'èxit del 50%.

Atac PTW (2007) per a 104 bits:
Amb 40.000 IV, probabilitat d'èxit del 50%.
Amb 60.000 IV, probabilitat d'èxit del 80%.
Amb 85.000 IV, probabilitat d'èxit del 95%.

3.2.2.5 Tècniques actives

En els atacs que cerquen l'obtenció de la clau WEP, sovint es combinen tècniques actives amb la captura de paquets del medi per tal de reduir el temps necessari per a obtenir els IVs suficients. Amb la *desautenticació* o

desassociació, es forcen a les estacions clients ja connectades a tornar-se a connectar i generar tràfic. Aquesta tècnica, que per si sola constitueix un atac de denegació de servei, té efectes visibles sobre la víctima.

Una altra tècnica és la *reinjecció de paquets*. Aireplay, la eina de reinjecció de la suite aircrack (que analitzarem més endavant) permet reinjectar en temps real tot el tràfic capturat de la xarxa forçant l'AP a reenviar paquets. En el cas que l'AP torni a xifrar els paquets (això no és sempre així) es generen nous IVs. També permet reinjectar un paquet ARP capturats (que es dedueixen per la seva mida fixa) el que força al AP a respondre (en aquest cas es produeixen continues peticions ARP vàlides i per tant un diàleg, no només un reenviament) amb nous IVs.

Donat que perquè l'AP accepti el paquets de l'atacant aquest ha d'estar associat, en els cassos de filtrat MAC l'atacant pot falsejar la seva pròpia MAC (amb programes com macchanger) suplantant un client legítim, i realitzar una *associació falsa* amb aireplay.

3.2.3 Trencament del xifrat WPA i WPA2

3.2.3.1 Atac intra-psk

Per explotar la vulnerabilitat PSK descrita a 3.1.7.1, i si coneixem la clau PSK, s'han d'obtenir els dos primers missatges del *4-way handshake* de la víctima amb l'AP. Qualsevol dispositiu pot escoltar el medi passivament per obtenir-les. Si la víctima ja està associada, es pot forçar un atac de desassociació (3.2.1.2) per a forçar-la a associar-se a través del *4-way handshake* de nou.

D'aquesta manera, es poden obtenir les claus PTK que garanteixen la confidencialitat entre l'AP i les STA per part d'una altra STA associada i que conegui la PSK.

3.2.3.2 Atac fora de línia per diccionari de les PSK a WPA i WPA2

Aquest atac descriu com obtenir una PSK basada en frase (que està composada per paraules que consten en un diccionari). És efectiu per a un atacant quan hi ha una sola PSK a l'ESS, i també per a un atacant intern quan hi ha PSKs úniques.

És en el propi estàndard 802.11i on s'apunta que les claus basades en frase de menys de 20 caràcters proveeixen un baix nivell de seguretat ja que són susceptibles d'un atac per diccionari. Per a realitzar aquest atac, s'ha de capturar el *4-way handshake* i donat que la conversió de PSK a PMK és coneguda, es pot realitzar un atac de força bruta per diccionari contra la PMK.

Aquesta vulnerabilitat no radica tant en el disseny del xifrat com en la implementació dels fabricants, els quals han fet molt poc per adreçar els problemes de les claus basades en frase amb eines pròpies.

3.2.3.3 Atac Beck-Tews a WPA

El 8 de novembre de 2008, Martin Beck i Erik Tews van publicar un atac contra TKIP. Aquest atac utilitza un ChopChop (una explotació de la vulnerabilitat 3.1.6.4, *debilitat del IV*¸ descrita per Korek) modificat, que permet el desxifrat de paquets individuals sense trencar la PMK, per atacar MIC.

Aquest atac pot recuperar la clau MIC i el text clar d'un paquet xifrat curt (e.g. un paquet ARP o DNS) i falsificar-lo utilitzant la clau recuperada. El temps d'execució de l'atac és entre 12 i 15 minuts. Donat que aquest atac està basat en l'atac per repetició (es dedueixen valors de la clau reenviant paquets modificats bit a bit per comprovar si l'AP els accepta), i que les contramesures que MIC implementa per aquest tipus d'atac (si es produeixen més de dos paquets erronis per minut la connexió es suspèn i les claus es canvien) les víctimes han de suportar les característiques QoS de 802.11e, de tal manera que l'atacant disposa de 8 canals simultanis per als que testejar MIC i pot obtenir un byte per minut. Si s'assumeix la xarxa IP de la víctima, per un paquet ARP nomes es desconeixen 13 bytes (1 de l'adreça IP del client, 8 de MIC i 4 de l'ICV), dels que s'obtenen els darrers 12 per Chopchop i el primer es calcula donat que ja es s'ha desxifrat els 4 bits de l'ICV.

Donada la vulnerabilitat de MIC vista a 3.1.7.2, podem obtenir-ne la clau invertint la funció. En aquest punt, podem injectar paquets vàlid als canals QoS. En el millor dels casos, es podem injectar fins a 7 paquets a la víctima, poden enverinar els catxés ARP o DNS, per tal de causar una denegació de servei o redirigir la víctima.

WPA2 no és susceptible a aquest atac en utilitzar CCMP, que utilitza AES per a la gestió de claus i la integritat

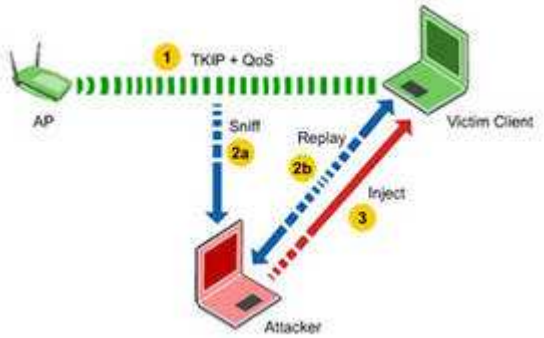

Fig. 3.5 Esquema de l'atac Beck-Tews

Al Juny del 2009, Finn Michael Halvorsen i Olav Haugen van descriure nous atacs a partir del Beck-Tews en un nou criptoanàlisis de TKIP.

Mesos després, Toshihiro Ohigashi and Masakatu Morii han descrit com aplicar el Beck-Tews a un atac MITM (*Man-In-The-Middle*) que redueix el temps de l'atac a un minut en el millor dels casos, i que permet atacar xarxes no QoS.

3.3 Conclusions

En aquest capítol hem realitzat una extensa cerca d'informació a Internet sobre les bases teòriques dels mecanismes de seguretat de WiFi, i els estudis que s'han realitzat sobre ella. Hem indagat quines són les tècniques que els atacants utilitzen per atacar a WiFi. Com ja ens imaginàvem, la majoria de la informació accessible fàcilment a Internet sobre seguretat WiFi està relacionada amb el trencament de claus de xifratge, amb l'objectiu de permetre a usuaris utilitzar sense consentiment la connexió a Internet d'un altre o penetrar en una xarxa sense autorització.

La gran quantitat de documentació que tracta el tema ens ha obligat a estendre l'estudi més del previst, ja que la motivació per obtenir la clau de xifrat ocupa la major part de documents, tècniques i eines dins de la seguretat WiFi. Aquestes tècniques cal conèixer-les, ja que tot i que en molts casos estan nomes pensades per obtenir la clau, són d'utilitat en altres àmbits de la seguretat WiFi, molts d'ells igual o més perillosos que l'obtenció il·lícita d'una clau de xifrat, com la denegació de servei o la intrusió no autoritzada amb diversos fins.

Tot i que aquesta és la principal motivació que s'amaga darrera de moltes de les pàgines que hem visitat, és molt interessant comprovar, a mesura que un s'endinsa en els inicis del *cracking*, com aquest s'alimenta d'estudis acadèmics d'una profunditat, coneixement matemàtic i professionalitat sorprenents. Si bé una de les bondats d'Internet és la de la accessibilitat de la informació, és impressionant la facilitat com es poden aconseguir guies i software que permeten el trencament de claus WEP de manera molt ràpida i relativament senzilla. Immediatament, és posa de manifest el grau de inseguretat del equipament que avui en dia els proveïdors d'accés a Internet instal·len als seus client, si bé aquest tema es tractarà més a fons en les conclusions finals del treball.

Però no tot és xifrat, i la quantitat de documentació relativa a seguretat Wireless des d'un marc ampli que contempli tots els perills que aquesta tecnologia comporta als usuaris és present, tot i que menor que la anterior. Aquí hi trobem un bon ventall de tècniques com la del Rogue AP o Man-in-the-Middle que permeten utilitzar la tecnologia WiFi per quelcom molt més perniciós que no pagar una connexió a Internet. Lluitar contra aquests atacs, especialment en entorns corporatius, és molt més complex que implementar un bon xifrat, sent l'únic considerat segur avui en dia WPA2 – enterprise.

Ara bé, coneixent a fons els diferents xifrats per a WLAN, aquests poden resultar més o menys adequats en funció de l'entorn (el que es considerarà i ponderarà arribat el moment). En el cas d'utilitzar WPA-PSK, s'ha de tenir en compte que la confidencialitat entre estacions és tan dolenta com a WEP, i que és un xifrat susceptible als atacs descrits al final de l'apartat 3.2.3.3 (atac Beck – Tews). Tot i així, si la PSK està composada per caràcters aleatoris i es canvia amb freqüència, el xifrat no està trencat. Cal tenir en compte però, que si la PSK és basada en frase i és menor de 20 caràcters, el risc d'utilitzar-la en WPA és major que utilitzar-la en WEP.

En aquest treball es respectarà la importància d'un bon xifrat, però donant-li el pes específic que li correspon dins del marc ampli de la seguretat WiFi.

4. CAPÍTOL 4. ANÀLISI

Finalitzat l'estudi de les bases teòriques, aquest capítol inicia el treball de camp amb la xarxa WiFi plantejant l'estratègia d'actuació, continua realitzant un anàlisi tècnic i una cerca de sistemes d'informació que desplegar a la xarxa, i acaba, amb els resultats d'aquestes dues accions, per refinar els objectius i la planificació del treball.

4.1 Escenari

El nivell de coneixement disponible de la xarxa WiFi per part del departament en el inici d'aquest treball és molt escàs. Es realitza un manteniment correctiu dels equips i dels sistemes, de tal manera que només es realitzen actuacions a partir de interrupcions en el servei. No es disposa de cap sistema de monitorització sobre l'equipament, el que provoca que no es conegui l'estat operatiu de la xarxa fins que l'usuari ho comunica.

Partint d'aquí, es plantegen dues línies paral·leles d'actuació que es mantindran fins a la fi del treball. Cada una d'elles consta de l'anàlisi, disseny i implementació d'una sèrie de mesures sobre la xarxa. La primera d'elles es centrarà en l'anàlisi tècnic per tal d'obtenir correccions a curt termini que millorin l'estabilitat del servei. La segona cercarà la construcció d'uns sistemes d'informació al departament que proporcionin serveis de monitorització, alertes i gestió d'esdeveniments (consulta, correlació,...).

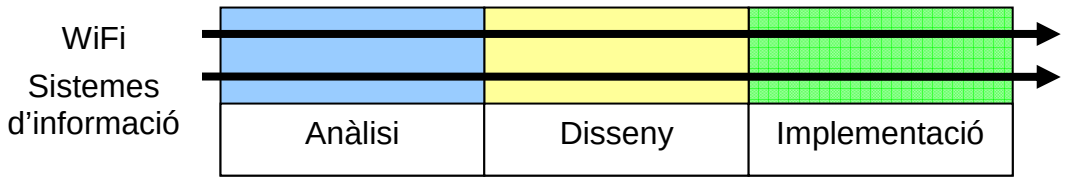

Fig. 4.1 Línies d'actuació

4.2 Anàlisi de la xarxa WiFi

La primera línia es centrarà en l'estudi de seguretat i la optimització de la xarxa WiFi, i culminarà amb l'execució de les pertinents correccions, si són necessàries, a curt termini.

Aquest anàlisi té com objectiu paral·lel a la implementació de les mencionades correccions ampliar el coneixement que es té sobre la instal·lació de xarxa.

Això es farà a través d'un estudi de camp sobre els següents aspectes de la configuració operativa:

4.2.1 Estudi de l'emplaçament

L'edifici de 9 plantes on es troba emplaçada la xarxa presenta una planta molt llarga (uns 40 m) i molt estreta (inferior a 10m) confrontant amb altres edificis.

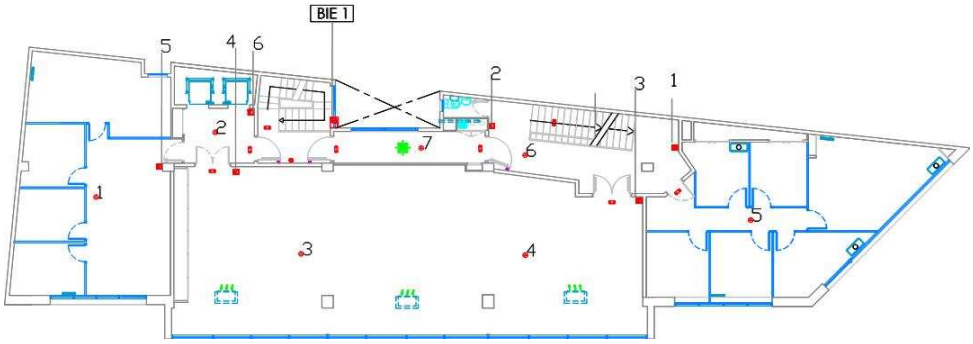

Fig. 4.2 Planta de l'edifici

Aquesta poca amplada ens permet simplificar la distribució dels punts d'accés (amb antenes omnidireccionals típiques) en aquesta dimensió, però presenta una dificultat si desitgem contenir la radiació de la senyal als límits físics de l'edifici. Els punts d'accés es troben situats a punts diversos de l'edifici, sense seguir cap estructura d'optimització de cobertura, fins al punt que en trobem un AP amb antena omnidireccional posicionat al cantó que uneix la paret que separa l'edifici del veí i la paret que dona al carrer, el que provoca que ¾ parts de la cobertura es radiessin a fora del límits (figura 4.3). Això és especialment crític donat que tal i com es veurà després la xarxa no està xifrada i presenta un gran nombre d'usuaris no autoritzats.

La posició dels APs suggereix que el seu desplegament s'ha fet a mesura que hi havia necessitats de cobrir noves àrees i que aquest ha estat limitat enormement pels indrets on es podia fer arribar alimentació elèctrica i cable Ethernet. Així mateix, detectem que els APs estan situats freqüentment en la mateixa ubicació en diferents plantes, el que provoca una mala distribució de la cobertura, solapant canals en punts on es troba una concentració vertical d'APs, i en zones amb baixa o nul·la intensitat de senyal ràdio.

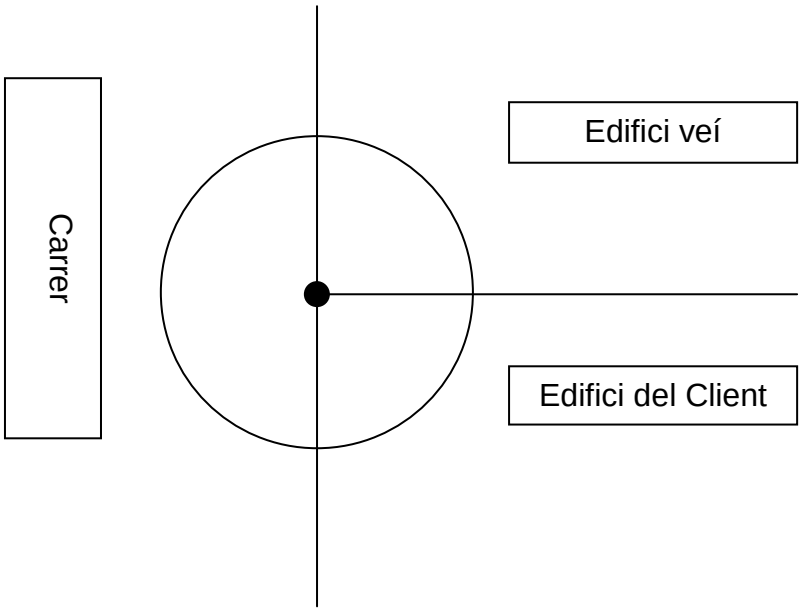

Fig. 4.3 Ubicació errònia d'un punt d'accés

4.2.2 Estudi de la topologia i adreçament IP

La xarxa WiFi que s'està estudiant presenta un topologia molt senzilla. La cobertura ràdio es proveeix amb 8 punts d'accés distribuïts en les 9 plantes de l'edifici, connectats a un DS Ethernet commutat que es concentra al *switch* de l'armari de comunicacions del DTI (Departament de Tecnologies de la Informació) seguint una clàssica topologia d'estrella. Aquest commutador Ethernet proporciona connectivitat a Internet a través d'un enllaç de les mateixes característiques dels anteriors (100 MB en estrella) que enllaça amb un *router* Ethernet, que al seu torn enllaça amb un *router* de fibra del ISP sobre el que no disposem de gestió.

Es disposa del següent mapa de xarxa, on es poden veure les dues xarxes IPs que configuren la xarxa WiFi.

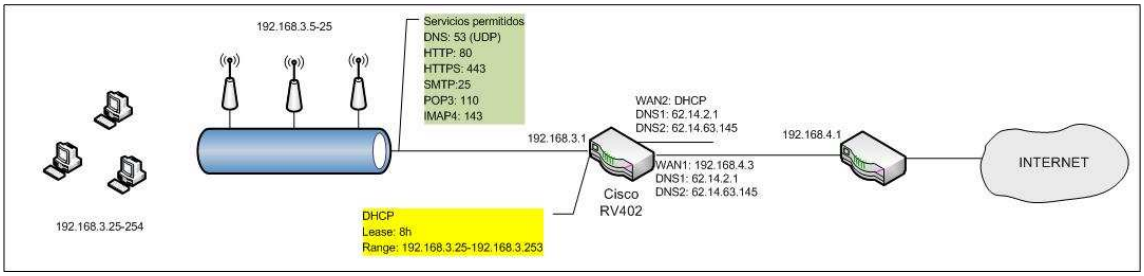

Fig. 4.4 Mapa de xarxa

La primera és la 192.168.3.0/24, on hi ha totes les adreces de gestió dels APs i el *switch* Ethernet que concentra el DS Ethernet, i sobre la que dóna adreces el DHCP als equips finals. Trobem tres conjunts d'adreces:

192.168.3.1-4: Equips d'electrònica de xarxa: *Router*, Gestió del *Switch*.
192.168.3.4-25: Punts d'accés configurats amb adreça fixa.
192.168.3.26-254: Conjunt d'adreces servides per DHCP.

4.2.3 Anàlisi del medi radio

En aquesta etapa s'ha analitzat el medi ràdio del edifici on la xarxa està situada. Es realitza un estudi de l'ocupació de l'espai radioelèctric en la banda dels 2.4 Ghz en els que opera la tecnologia WLAN. Per a aquest anàlisi comptem amb un portàtil amb un adaptador WiFi, i del software inSSIDer.

Els resultats han estat:

- Trobades tres antenes Yagi connectades a APs de les que el departament no en tenia coneixement, en els falsos sostres.
- Detectat mal funcionament d'un AP.
- Detectat solapament de canals entre dos BSS.

Tota la informació dels canals 802.11 recopilada s'ha actualitzat al mapa de xarxa.

4.2.4 Configuració dels punts d'accés

S'ha revisat la configuració operativa dels diferents punts d'accés que configuren la xarxa WiFi. S'analitzaran paràmetres de configuració ràdio, xarxa, seguretat i de gestió, i es comprovarà que els equips disposin del últim firmware disponible pel fabricant. També s'han estudiat les característiques pròpies de cada AP.

4.2.5 Elaboració d'un mapa de cobertura

Per tal de treballar visualment sobre la cobertura, s'ha elaborat un esbós a mà que il·lustra la disposició física del punts d'accés i dels canals ràdio que s'utilitzen en l'edifici, indicant la zona de cobertura que proveeixen. Aquest mapa ens ha permès identificar zones amb cobertura solapada de diversos APs, zones sense cobertura, i ens ha ajudat a optimitzar els canals ràdio 802.11. Donat que la planta de l'edifici és molt estreta (figura 4.2) i per tant en cap cas tindrem més d'un AP en la seva amplitud, hem pogut menysprear una de les dimensions físiques i treballar únicament amb l'alçat de l'edifici, el que ha

revelat la importància de tenir en compte l'alçada en aquest tipus de plantejaments, ja que la radiació d'un AP sovint afecta als pisos pròxims.

4.2.6 Anàlisi de tràfic

Finalment, es realitzarà un breu anàlisi de tràfic en situació d'operativitat i de no operativitat per tal de detectar la font o fonts del problema. Es troben quantitats importants de tràfic mal format. A la xarxa en aquest moment hi ha dos tipus diferents d'APs. Gran part d'ell prové d'un d'ells.

4.2.7 Monitorització

A l'espera de desenvolupar els sistemes d'informació, hem començat a monitoritzar la connectivitat dels punts d'accés amb pings continus i s'han efectuat supervisions de les connexions actives y correlacions amb el número de *leases* del servidor DHCP de la xarxa. Aquestes concesions indiquen clarament la presència d'un número anormalment gran d'usuaris a la xarxa, és a dir, usuaris no autoritzats, que estan tenint un impacte sobre el rendiment i la disponibilitat de la xarxa.

4.2.8 Avaluació de seguretat

S'ha realitzat una petita avaluació de seguretat a la xarxa. L'estratègia d'auditoria ha estat de tàndem (interna o de caixa de vidre), ja que el departament ha col·laborat amb l'auditor amb l'objectiu d'obtenir un punt de partida sobre el que treballar.

Taula 4.1 Resultats de l'avaluació

Seguretat WiFi		
Ràdio	**Enllaç, Xarxa i Transport**	**Altres**
Important radiació de senyal fora de l'edifici.	No hi ha xifrat.	No hi ha cap sistema de monitorització ni IDS (sistema de detecció d'intrusions).
	No hi ha filtrat de tràfic entre estacions.	
L'espectre WiFi dins de l'edifici està contaminat per múltiples xarxes veïnes.	No hi ha filtrat del tràfic de gestió en els APs (aquests són atacables pels usuaris).	
	Hi ha filtrat del tràfic sortint per permetre 6 serveis: DNS, HTTP, HTTPS, SMTP, POP3 i IMAP4.	
	Les contrasenyes de gestió són bàsiques i iguals per tots els APs.	

4.3 Anàlisi de la implementació de sistemes d'informació

La segona línia tindrà com a objectiu la instal·lació permanent d'una arquitectura de sistemes de informació que ajudi a aconseguir:

- Millorar la qualitat de servei.
- Millorar la resposta de l'equip tècnic a incidents.

Els sistemes d'informació han de permetre:

- Recopilar els *logs* dels diferents dispositius de la xarxa.
- Monitoritzar els dispositius en temps real.
- Correlar successos en el temps.
- Detectar comportaments anòmals.
- Obtenir alertes primerenques.
- Executar eines amb rapidesa des d'una ubicació centralitzada.

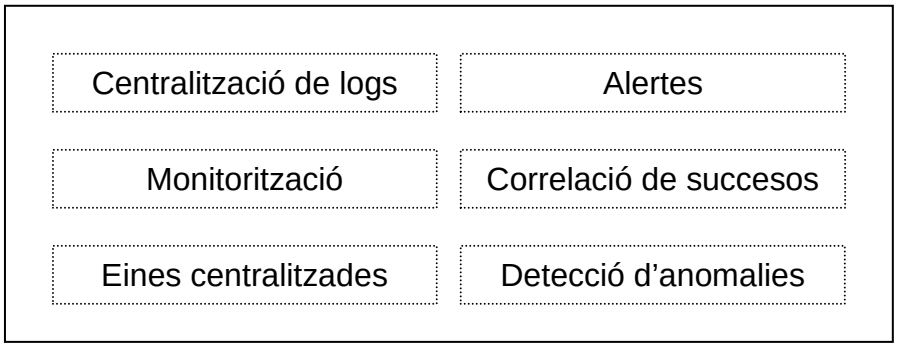

Fig. 4.5 Components de l'arquitectura

4.3.1 Cerca i selecció de sistemes d'informació

Per tal de poder acomplir els objectius llistats, s'estudiaran en una primera etapa quines eines gratuïtes (requisit de la institució) són les més adequades.

Així doncs, s'ha realitzat una cerca de *software* sense cost (requisit del client, en la majoria dels casos hem optat doncs per solucions de codi obert) a Internet que ens permeti, totalment o en part, assolir els objectius esmentats en l'apartat anterior. D'aquesta cerca han resultat els següents candidats:

- NST (http://networksecuritytoolkit.org/)
- NAGIOS (http://www.NAGIOS.org/)

- Zenoss Core (http://www.zenoss.com/)
- OSSIMM (http://www.alienvault.com/products.php?section=OpenSourceSIM)

Aquests candidats seran instal·lats en màquines virtuals per tal d'avaluar-los en l'entorn de producció real.

4.4 Refinament

4.4.1 Refinament d'objectius

Arribat a aquest punt on s'ha estudiat la base teòrica i s'ha analitzat la xarxa, tornem a revisar els objectius del treball per tal de valorar-los i refinar-los si s'escau:

O1. A través de l'estudi dels capítols 2 i 3 s'ha ampliat el coneixement de seguretat WiFi suficientment com per encarar el treball. S'ha assolit aquest objectiu.

O2. Donat que en el capítol 2 s'ha estudiat l'auditoria tècnica de seguretat de manera suficient com per extreure un mètode d'anàlisi, s'ha assolit aquest objectiu.

O3. Tal i com hem planificat, la cerca i l'anàlisi de les eines es fa en paral·lel a l'estudi de WiFi i l'anàlisi de la xarxa. Els resultats d'aquesta cerca i anàlisi es situen en el començament del proper capítol per motius d'ordre, tot i que ja han estat obtinguts, pel que aquest objectiu ja s'ha assolit.

O4. Donat que en el capítol 3 hem realitzat l'anàlisi de la xarxa i n'hem extret dades sobre les que treballar, s'ha assolit aquest objectiu.

O5. La transmissió de coneixement es durà a terme principalment a través de sessions de formació i elaboració de documentació. Els 4 primers objectius permeten tenir tota la informació i dades necessaris per a aquestes actuacions.

O6. Aquest objectiu, encara no assolit, pot desgranar-se en els següents:

O6.1 Augment de la disponibilitat (*uptime* o temps de servei) a través d'incrementar la seguretat i dissenyar i executar aquelles millores tècniques que s'estimin adients.

O6.2 Minimització del temps d'aturada (*downtime* o interrupció del servei). Això s'ha aconseguirà a través de:

1. Augment de la capacitat de resposta davant d'incidències i caigudes de serveis. Per tal de aconseguir-lo és dotarà de més coneixement i més eines al departament.

2. Desplegament de sistemes de monitorització i alertes que permetin conèixer més ràpidament i profunda els esdeveniments dels sistemes.

3. Implementació d'un sistema de correlació d'esdeveniments que ens ajudi en l'anàlisi de situacions.

O7. Donat que aquest treball és un exercici real, s'avaluaran les millores efectuades des d'un punt de vista acadèmic així com dels beneficis concrets percebuts per l'empresa.

4.4.2 Refinament de tasques

- Disseny d'accions correctives.
  - Disseny d'una arquitectura formada pels sistemes d'informació ja seleccionats per a la seva implementació a llarg termini. **20 hores**.

- Implementació de les mesures dissenyades.
  - Execució de les mesures correctives a curt termini. **20 hores**.
  - Implementació d'una arquitectura de sistemes d'informació. **60 hores**.

- Valoració dels resultats i estudi de línies futures.
  - Valoració del compliment de: **6 hores.**
    - Objectius
    - Planificació
    - Costos
    - Beneficis per l'empresa
  - Descripció de línies futures d'investigació i desenvolupament. **2 hores.**

4.4.3 Reestimació de la planificació i els costos

Pels motius exposats a les conclusions del capítol 3, s'ha produït una desviació del 3% en l'acompliment actual de la planificació, en realitzar-se 8 hores més de les previstes, el que repercuteix en la mateixa proporció amb els costos actuals del treball.

5. CAPÍTOL 5. DISSENY

En aquest capítol s'analitzen les eines i els sistemes d'informació que s'utilitzaran per a aplicar correccions en el proper capítol sobre els resultats obtinguts amb l'anàlisi prèvia.

5.1 Estudi d'eines de seguretat WiFi

Per tal de poder dur a terme l'anàlisi de la xarxa WiFi, s'ha fet una recerca d'eines.

En primer lloc, s'han estudiat diferents distribucions Linux que es troben gratuïtament a Internet creades específicament per a la auditoria WiFi. L'annex 1 recull una taula amb aquesta comparativa.

De les 7 distribucions analitzades, destaquem Wifislax i Backtrack, per ser les més completes, actualitzades, i que suporten una bona diversitat de targetes de xarxa.

Hem inclòs KCPentrix tot i ser una distribució pensada per a fer tests de penetració en un àmbit molt més ample que en el de WiFi, per ser la distribució més completa que hem trobat, i que cal tenir en compte en cas que per fer l'auditoria es necessiti una eina que no es trobi al domini de les distribucions d'auditoria WiFi (anomenades també auditoria *Wireless*), que sovint han estat creades amb l'única intenció d'aconseguir trencar el xifrat.

S'han considerat com a paràmetres per a la comparativa:

- Facilitat de transport: Donat que l'auditoria es realitza generalment des de diverses ubicacions físiques.
- Disponibilitat: Entesa com a la rapidesa en que el *toolkit* pot estar operatiu.
- Cost econòmic.
- Consideracions tècniques: Aquí hem considerat diversos aspectes funcionals com els requeriments dels equips necessaris i possibles limitacions o avantatges de la opció estudiada per al *software*, com la possibilitat d'escriure a disc tot allò que l'estudi de la xarxa generi.

En segon lloc, s'han cercat i avaluat eines especifiques per a tot allò que no quedava cobert per les distribucions.

5.1.1 Format d'execució

S'han analitzat les següents opcions d'execució, per tal de trobar-ne una que ens permetés el màxim de flexibilitat en termes de mobilitat i disponibilitat, necessaris a l'hora de estudiar la xarxa WiFi.

- *Live* CD
  - Avantatges:
    - Medi econòmic i fàcil de transportar.
    - Redundància i escalabilitat: Es poden portar diversos dispositius per si un falla. Poden preparar-se diversos dispositius sense un cost econòmic significatiu.
    - Disponibilitat: el sistema operatiu es carrega en poc temps.
  - Desavantatges:
    - Necessita que l'equip disposi d'unitat lectora i que en suporti l'arrencada.
    - No permet l'escriptura d'arxius, necessitant una segona unitat externa o l'ús del disc dur del equip.
    - Espai de la distribució limitat al tipus de disc utilitzat.

- *Live* USB
  - Avantatges
    - Medi molt fàcil de transportar.
    - Permet l'escriptura d'arxius en el mateix dispositiu.
    - Redundància i escalabilitat: Es poden portar diversos dispositius per si un falla. Poden preparar-se diversos dispositius amb un cost econòmic moderat.
    - Disponibilitat: el sistema operatiu es carrega en molt poc temps.
  - Desavantatges
    - Necessita que l'equip suporti l'arrencada des del dispositiu.

- Màquina Virtual
  - Avantatges
    - Permet utilitzar el *toolkit* en diversos sistemes operatius sense la instal·lació d'un de nou.
    - Permet la multitasca amb altres aplicacions del sistema operatiu en que s'executi la màquina virtual.
    - Escalabilitat.
  - Desavantatges
    - Mala disponibilitat: Obliga a la instal·lació del *software* de virtualització.
    - La utilització de dispositius virtuals no permet la utilització d'eines de baix nivell necessàries per a determinats aspectes de l'auditoria.

Per un altre banda, també s'ha analitzat els pros i contres de concebre un *toolkit* com a la unió de la distribució i un PC portàtil:

- Instal·lació en disc

- Avantatges
  - No necessita de dispositius externs, fent l'equip més compacte i robust.
  - Permet escollir el *hardware* més adient per a la auditoria.
  - Permet la personalització total de la distribució al *hardware* del equip.
  - Permet l'escriptura de fitxers a disc, amb un espai generalment major que en els dispositius externs estudiats (no és així en el cas d'un HD extern).
- Desavantatges
  - El PC passa a formar part del *toolkit* convertint-lo en una eina costosa, pesada i voluminosa.
  - No proporciona redundància si l'equip falla.
  - Poc escalable econòmicament, ja que es necessita un equip per cada tècnic que realitzi la auditoria.

5.1.2 Estudi d'eines especifiques

Un cop examinades les possibilitats del que ofereixen les diferents distribucions, hem fet una recerca d'eines que aportessin noves formes d'auditar una xarxa WiFi, o que cobrissin aspectes no coberts per la distribució. Els annexos 2 i 3 contenen un llistat d'aquestes eines i un quadre comparatiu d'eines de descobriment. D'aquesta recerca, ha sorgit inSSIDer de MetaGeek, un *stumbler* WiFi que utilitza la API de Windows, el que el fa molt independent dels controladors de dispositius. És una eina gratuïta, lleugera i amb una excel·lent interfície que ens mostra gràficament les xarxes del entorn. Tot i disposar d'eines similars com Kismet o Airodump, inSSIDer ha estat la eina utilitzada per al treball en el medi ràdio.

5.1.3 Conclusions

Per al treball amb les distribucions de seguretat, la utilització d'un PC dedicat esdevé en la gran majoria d'auditories un requisit. Això és així per qüestions de mobilitat, de necessitat d'un *hardware* específic i de seguretat. És important en les auditories que contemplin nivells inferiors al de xarxa que sigui el propi auditor qui tingui flexibilitat per escollir la eina *hardware* més adequada. Per altra banda, que l'auditor utilitzi els seus propis equips garanteix la privacitat dels mètodes i dades obtingudes en l'auditoria, sent això necessari en determinades estratègies d'auditoria.

En aquests casos, la millor opció en tots els aspectes es l'execució d'un *toolkit* ja instal·lat localment en el PC del auditor, per motius de ràpid desplegament i robustesa, al proveir a l'auditor d'un equip propi, independent del auditat, que ja ha estat verificat prèviament.

Ara bé, en determinats casos, pot ser necessària, més ràpida i molt útil la utilització d'un *toolkit* en un medi extraïble que pugui ser executat en un equip determinat. De les tres alternatives estudiades, la màquina virtual és descartada per la seva incompatibilitat amb la majoria de les eines necessàries per a l'auditoria, ja que no permet treballar directament sobre el *hardware* a menys que es tracti de dispositius USB, el que obliga a la utilització d'una tarja WiFi USB compatible amb les eines. La unitat USB en presentar els menors inconvenients es torna la millor alternativa així com per la seva versatilitat, preu, capacitat i major resistència física.

5.2 Estudi de sistemes d'informació

5.2.1 Introducció

Per cada un dels sistemes a avaluar, hem procedit per una banda a l'estudi de la documentació i recursos disponibles a Internet, i per l'altra hem realitzat instal·lacions de prova en màquines virtuals en l'entorn real de producció. El nostre entorn de virtualització està basada en VMWare ESXi a sobre d'un *hardware* Dell Equallogic. Aquest sistema permet fer *snapshots* de les màquines virtuals en diferents moments del temps, el que ens és de gran utilitat durant les proves. La virtualització també ens permet moure una màquina de l'entorn de producció real a un de test i vice versa amb molta rapidesa i comoditat.

5.2.2 NST

5.2.2.1 Introducció

NST és un *Toolkit* d'eines de seguretat de xarxa. Ens ha cridat la atenció la seva excel·lent integració d'elles en una WUI (*Web User Interface*).

5.2.2.2 Instal·lació

Aquesta distribució basada en Fedora pot ser executada en Live CD o en format de màquina virtual.

Hem pogut transferir aquesta màquina virtual al nostre entorn de virtualització amb facilitat, pel que ha estat el format de instal·lació escollit.

5.2.2.3 Característiques

L'operació habitual d'aquesta distribució és a través d'una WUI (*Web User Interface)* que ens ha permès desplegar NST fàcilment a la xarxa. Ens ha sorprès l'enorme nivell d'integració del WUI amb el sistema operatiu, i la profunditat de les operacions possibles a través d'ella. En realitat, no cal fer servir una consola en pràcticament cap ocasió.

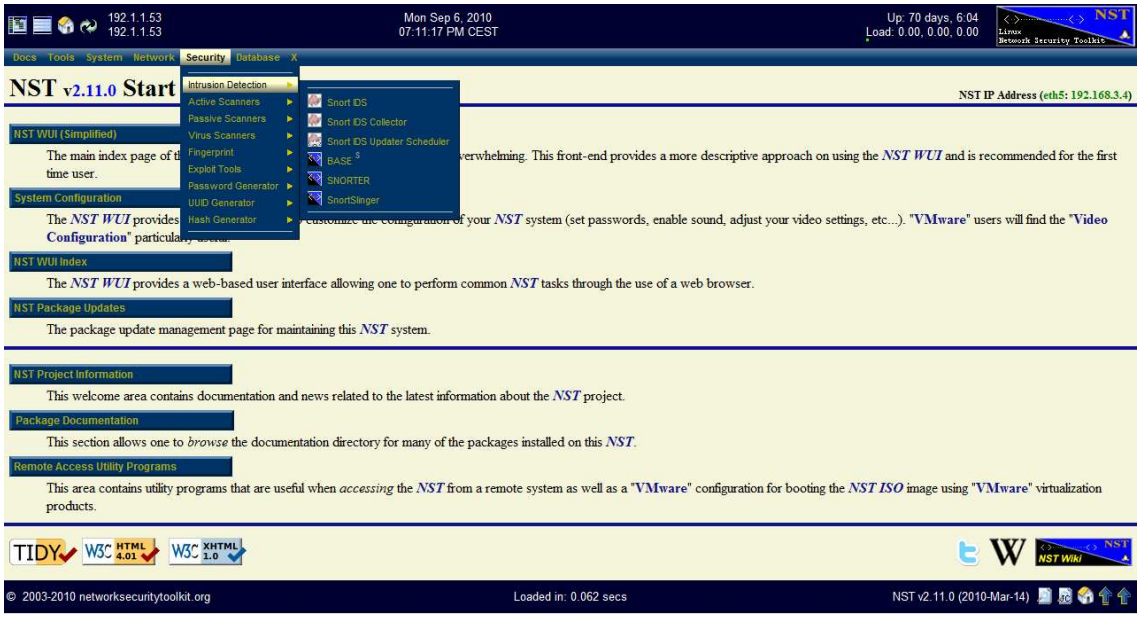

Fig. 5.1 WUI de NST

5.2.2.4 Conclusions

NST presenta una bona col·lecció d'eines de xarxa, de seguretat i WiFi, entre d'altres. Integra de manera molt destacable totes les eines en una amigable interfície web, el que facilita i fa més ràpides les operacions amb les eines.

5.2.3 NAGIOS

5.2.3.1 Introducció

NAGIOS és un dels sistemes més coneguts i utilitzats pel que fa a la monitorització. Presenta una interfície web per a la gestió dels dispositius i els esdeveniments lligats a ells.

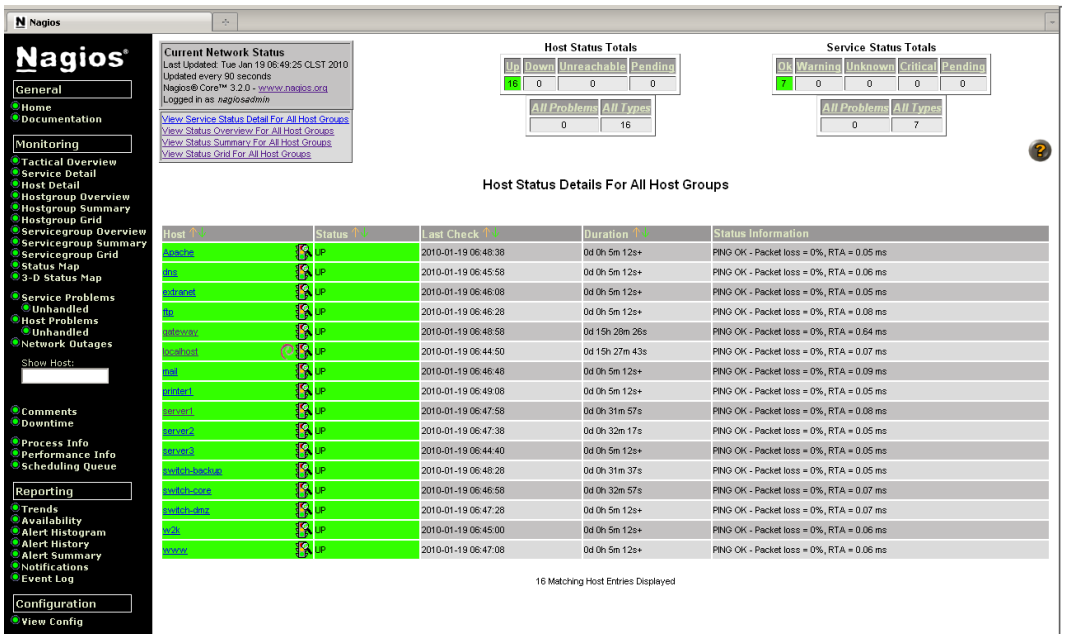

Fig. 5.2 Exemple de la interfície web de NAGIOS

És capaç d'enviar alertes i generar informes dels successos. Incorpora *event handlers* que són capaços de reaccionar davant d'un esdeveniment, per exemple, reiniciant un servei. També pot fer monitorització remota a través de túnels SSH o SSL.

5.2.3.2 Instal·lació

La instal·lació ha presentat una dificultat mitjana, ja que obliga a la compilació des del codi font. Això implica preparar el sistema, pel que la instal·lació és llarga. Primer s'han d'instal·lar els prerequisits (Apache 2, PHP, GCC i GD) i crear el compte i grup d'usuari. Seguidament s'ha de compilar, configurar l'interfície web a Apache, i configurar els *plugins*. Tot i les guies disponibles, ens hem trobat problemes no documentats amb una màquina Linux *out-of-the-box* (recent instal·lada).

5.2.3.3 Configuració

La configuració dels dispositius es fa editant arxius de text i scripts. Un cop configurats, els dispositius s'operen a través de la interfície web, tot i que moltes de les accions s'han de fer per comandes en un terminal. Es pot obtenir un mapa de dependencies dels dispositius, però les icones s'han de descarregar i instal·lar.

NAGIOS disposa de multitud de *plugins* i *addons*. Gràcies a ells, es poden monitoritzar dispositius per SNMP i WMI, i es poden generar gràfiques dels recursos, tot i que una solució molt comuna és utilitzar la eina RRD-Tool Cacti.

Així mateix, hi ha *software* creat per a complementar NAGIOS en algun aspecte (Splunk, per exemple, un *software* de cerca que ajuda a trobar la causa d'un succés).

5.2.3.4 Conclusions

Tot i que la potència i possibilitats del programa són inqüestionables i la operativa Web un cop configurat es força amigable, la seva complexitat d'instal·lació, configuració i administració dels dispositius i mòduls d'aplicació (siguin *plugins* o *addons*) fa que el sistema hagi de ser operat per personal amb un nivell alt de coneixement i preparació, el que no fa NAGIOS un bon candidat per l'entorn on ens trobem.

5.2.4 Zenoss

5.2.4.1 Introducció

Zenoss és una solució de gestió IT de codi obert. Permet gestionar l'estat de la infraestructura IT a través d'una única interfície web, que treballa sobre una base de dades que conté l'inventari de dispositius, creats a través d'un procés de descobriment. Zenoss monitoritza aquests dispositius, generant esdeveniments vinculats i característiques de gestió de fallada. Aquestes característiques ajuden a la productivitat ja que automatitzen la notificació, alertes, escalatge i tasques de remei diàries.

5.2.4.2 Instal·lació

La instal·lació presenta un dificultat baixa. Està disponible un *stack installer* que permet la instal·lació sense prerequisits *software*. El *stack* incorpora mysql, servidor web,... tot integrat i llest per executar un cop instal·lat.

Dels múltiples mètodes d'instal·lació que ofereix, hem escollit en una primera instància la màquina virtual. Una vegada funcionant, hem comprovat que aquesta màquina porta un sistema operatiu CentOS. Donat que aquest no ens atreia per a implantar-lo, degut al desconeixement d'aquesta distribució al departament, decidim provar el *stack installer* a sobre d'una màquina virtual en la que hem instal·lat Ubuntu server.

La configuració dels dispositius es fa mitjançant interfície, o a través d'autodescobriment.

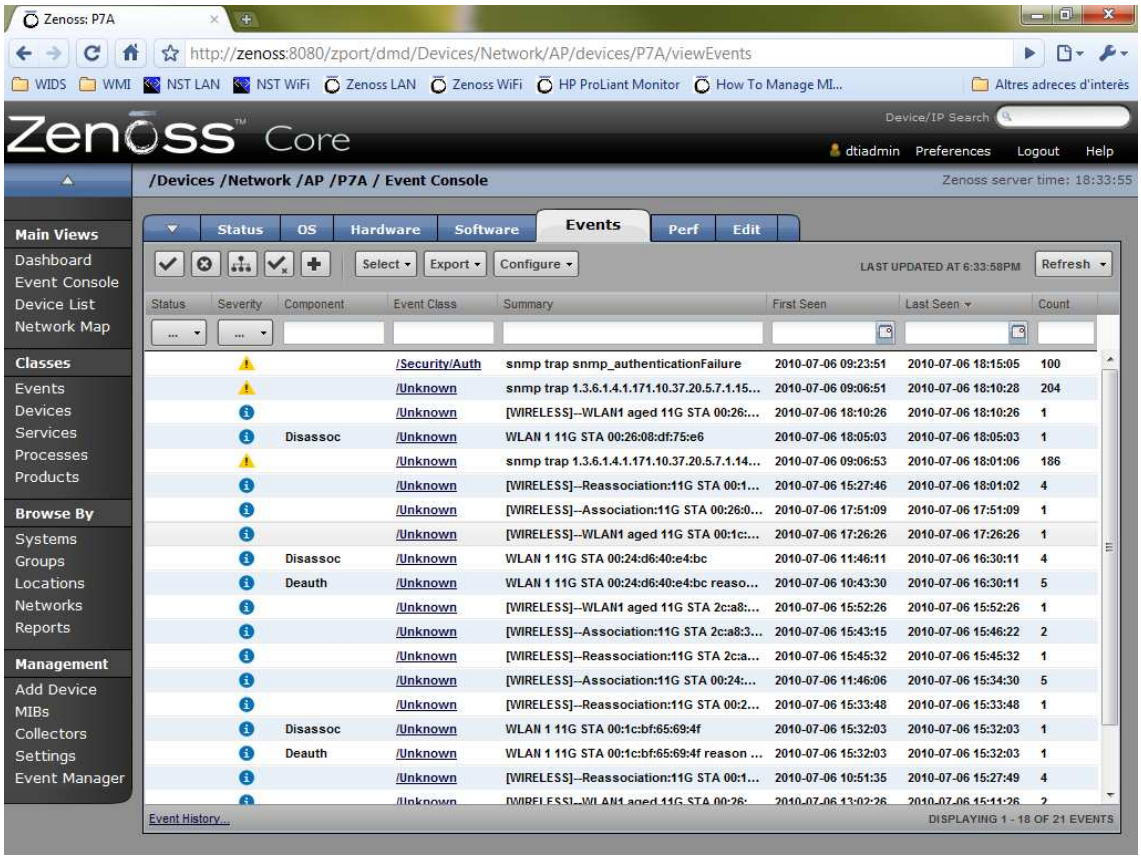

Fig. 5.3 Esdeveniments d'un AP a Zenoss

5.2.4.3 Característiques

Zenoss ha estat dissenyat amb els següents principis:

- Modelatge: El sistema pot determinar com monitoritzar l'entorn en el que es troba. El model està basat en objectes, i és fàcilment escalable a través d'herència.
- Descobriment: El sistema interroga cada dispositiu per recopilar-ne informació detallada.
- Normalització: La informació provinent de diferents fonts (e.g. Windows, Linux) és presentada de la mateixa manera.
- Recopilació de dades sense agent: La comunicació amb els dispositius es realitza a través de diversos protocols (SNMP,SSH,Telnet i WMI).
- Infraestructura IT completa: L'abordatge del sistema inclou totes les àrees: xarxa, servidors i aplicacions.

- Herència de configuració: Els paràmetres de configuració central (*zProperties*) i les directrius de monitorització (*monitoring templates*) utilitzen herència per a definir com es monitoritza un dispositiu.

- Monitorització inter-plataforma: El sistema monitoritza diversos sistemes operatius, dispositius amb SNMP, i diverses aplicacions software.

- Escalabilitat: El sistema es pot desplegar en un sol servidor per a gestionar centenars de dispositius. Si un de sol no és suficient, o si volem monitoritzar dispositius en diferents xarxes o localitzacions, es poden desplegar col·lectors que arrepleguen les dades de forma distribuïda concentrant la monitorització en un sol sistema Zenoss.

- Extensibilitat: El mecanisme d'extensió del sistema, els ZenPacks, permeten addicions i modificacions ràpides per a personalitzar l'entorn.

Destaquem les dues següents característiques:

- De-duplicació: Aquesta característica permet que els esdeveniments que es repeteixin es mostrin un sol cop en la interfície, passant a ser el número de cop que han succeït una propietat més.

- Auto-Neteja: Aquesta característica que només aplica en esdeveniments generats pel propi Zenoss, permet que un esdeveniment sigui esborrat quan el seu oposat succeeix, *e.g.* dispositiu operatiu esborra a dispositiu caigut.

La informació arriba a Zenoss per un dels seus múltiples *daemons*, que es divideixen en aquells que activament recopilen dades i aquells que les capturen o les reben:

Daemons de generació d'esdeveniments:
- *zenping* – Esdeveniments de ping *up/down.*
- *zenstatus* – Esdeveniments de port TCP *up/down.*
- *zenperfsnmp* – Esdeveniments d'agent SNMP *up, down* o umbral.
- *zencommand* – Esdeveniments d'estat genèric obtinguts per comandes (*e.g.* SSH), umbral.
- *zenprocess* – Esdeveniments de procés *up, down* o umbral.
- *zenwin* – Esdeveniments de servei de Windows *up/down.*

Daemons de captura d'esdeviments:
- *zensyslog* - Esdeveniments obtinguts dels missatges de *syslog*.
- *zentrap* - Esdeveniments creats des dels *traps* i *informs* SNMP.
- *zeneventlog* - Esdeveniments extrets del registre d'esdeveniments de Windows.

Zenoss diferencia entre les dues principals tècniques de monitorització: disponibilitat i rendiment (figura 5.4). La primera vigila constantment els dispositius per tal de generar alertes quan el seu funcionament és erroni. La

segona recull dades sobre diferents paràmetres de rendiment dels recursos la màquina (CPU, memòria,...) en el temps, i en genera unes gràfiques temporals.

Zenoss suporta de manera nativa la monitorització gràfica de rendiment en sistemes Linux. Pot ser estesa amb *Zenpacks* (plugins que desenvolupa la comunitat) per tal de monitoritzar processos Java, servidors web Apache, *hardware* Dell, HP, i virtualitzat amb VMware, entre molts més. Amb aquests plugins, i a través de SNMP o WMI, s'aconsegueix accedir a dades de més sensors del *hardware* d'un sistema en concret (e.g. revolucions dels ventiladors o nivells de tensió de la font d'alimentació).

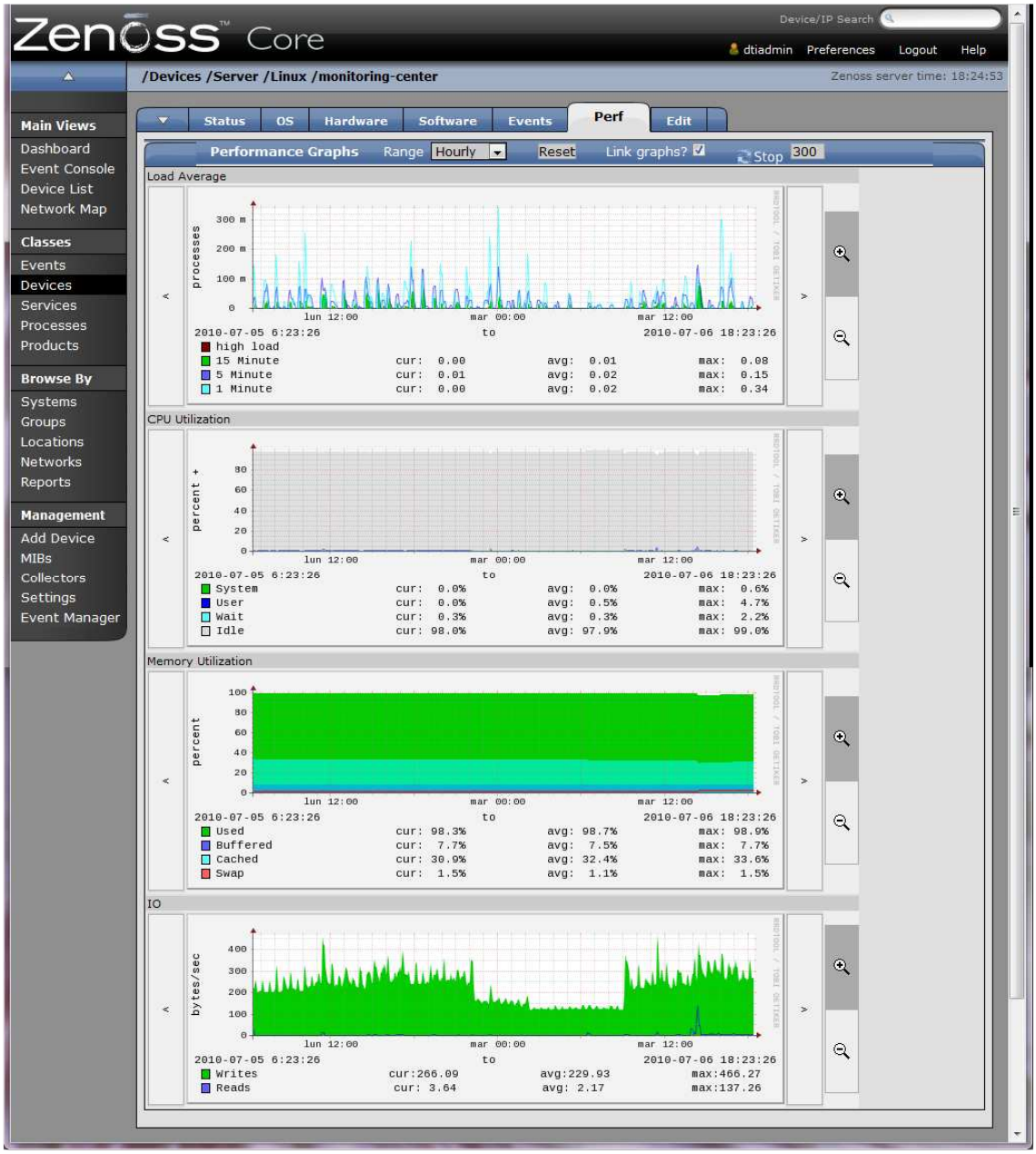

Fig. 5.4 Gràfiques de rendiment d'un servidor

La monitorització de rendiment nativa en Windows és fa a través de *snmp-informant* (*software* de tercers), o un *Zenpack* que no necessita d'aquest agent, però que necessita els paquets snmp i bc a la màquina Linux on corre el Zenoss. Comparant-los, *snmp-informant* captura informació del hardware, concretament dels discs durs, que el *Zenpack* no dóna. També dóna informació de rendiment del *paging*.

Una altra alternativa per a la monitorització de rendiment és a través de WMI (*Windows Management Instrumentation*) amb el corresponent *zenpack*. Amb WMI, no cal instal·lar cap servei ni cap agent a la màquina, la profunditat de monitorització és major i la seguretat és millor i està integrada amb Windows. L'únic inconvenient és que si s'utilitza el tallafocs integrat de Windows la configuració és un pas més complicada que amb SNMP, però en general la addició d'un dispositiu al sistema és molt més ràpida.

El sistema permet que un dispositiu estigui organitzat de diverses maneres: una classe (obligatori), una ubicació, un grup de dispositius i un servei. D'aquí pengen diverses parts del sistema, com les *zProperties*, plantilles de rendiment i comandes. Els informes permeten filtrat a través dels organitzadors.

Així mateix, es disposa de característiques avançades que van més enllà de la monitorització i la creació d'alertes i d'informes. El modelatge permet la recopilació automàtica d'informació d'un dispositiu. Aquesta funció és molt potent quan no s'utilitza un agent. Per altra banda, la de-duplicació i l'auto-neteja funcionen de manera intel·ligent i ajuden a identificar esdeveniments particulars.

5.2.4.4 Conclusions

Zenoss ens ha resultat excel·lent com a eina de monitorització, gràcies a la seva interfície basada en Zope, i les característiques avançades. Fa una excel·lent classificació de dispositius i recopilació d'informació. El modelatge automàtic i periòdic permet tenir sempre actualitzada la base de dades de dispositius, podent substituir així a qualsevol base de dades d'inventari. A partir de les dades sobre la configuració de xarxa dels dispositius, Zenoss elabora automàticament un mapa de xarxa de nivell 3 força senzill, encara que funcional i amigable (figura 5.5).

Pel que fa a la correlació d'esdeveniments, Zenoss no va més enllà de ser un excel·lent sistema de monitorització, tot i que les funcionalitats de *deduplication* i *auto-clear* són un pas en aquesta direcció i simplifiquen molt la tasca d'una eventual correlació manual.

Aquest *software* disposa d'un gran suport de la comunitat i filosofia de codi obert. És fàcilment ampliable, integrable i configurable a mida. Hi ha *Zenpacks* per a *hardware* específic: HP, Dell, APC,... (figura 5.6).

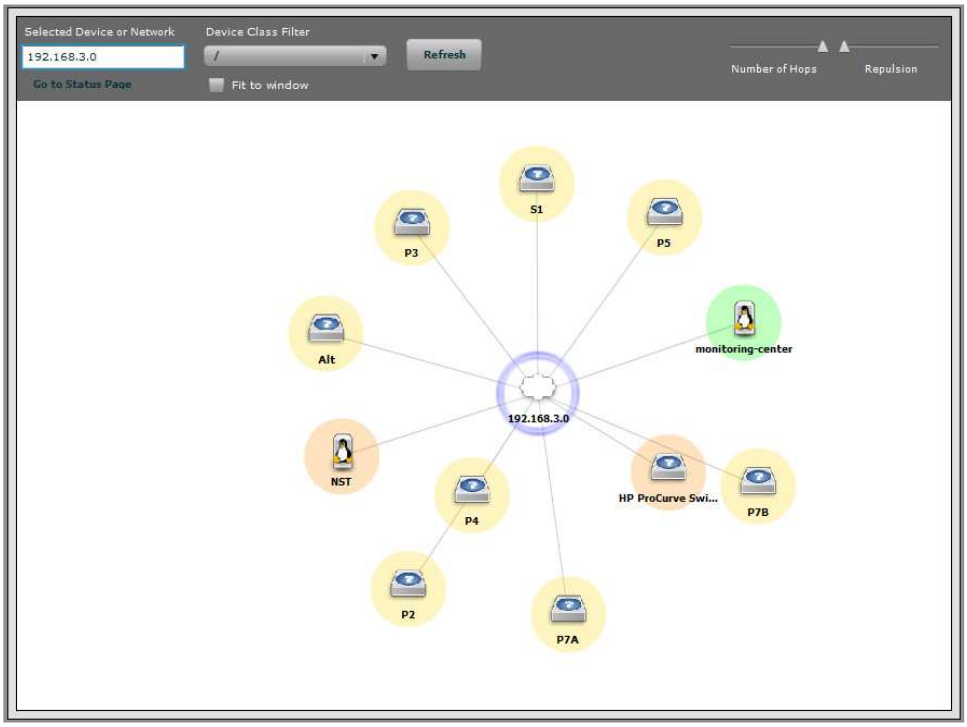

Fig. 5.5 Mapa de xarxa IP integrat

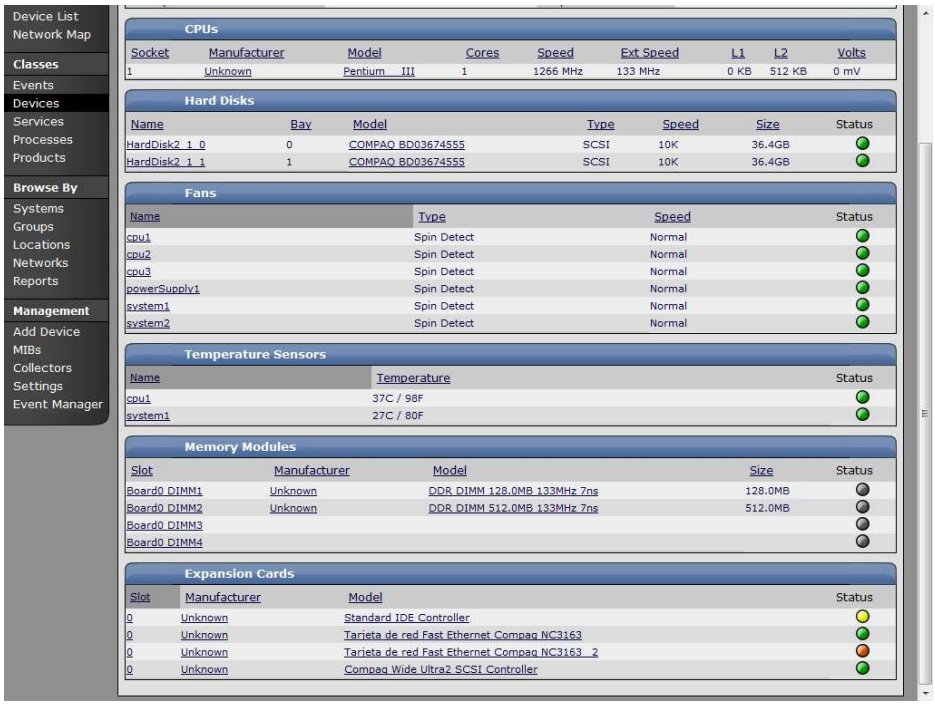

Fig. 5.6 Pestanya *hardware* d'un dispositiu HP amb agents del fabricant

5.2.5 OSSIM

5.2.5.1 Introducció

OSSIM es presenta com una enorme *suite* de codi obert d'eines de seguretat i correlació d'esdeveniments. De manera anàloga a NST, incorpora un tot el *software* integrat accessible a través d'una interfície web.

5.2.5.2 Instal·lació

Hem procedit a la instal·lació del sistema en un màquina virtual sense sistema operatiu, tal i com s'indica. El fet de que OSSIM es distribueixi com una distribució sencera per instal·lar en una màquina sense sistema operatiu ja en dóna una idea de les dimensions del sistema. La instal·lació és fàcil, però seguidament hi ha una preconfiguració del sistema en la que es demana, entre d'altres:

- Tria dels components del sistema
- Seleccionar xarxes en mode promiscu
- Xarxes a monitoritzar
- Proxy
- Selecció de plugins, sondes, ...

En el punt de test del sistema en que es trobem, no sabem respondre encara a moltes d'aquestes preguntes. Tot i així, finalitzem la configuració i podem accedir al sistema. Després de haver-lo provar, hem arribat a la conclusió que és un sistema molt gran, extens i complet, que excedeix les necessitats del entorn en que ens trobem.

Per una banda, algunes de les funcions que ens cridaven més la atenció d'aquest sistema, com la correlació d'esdeveniments, només estan disponibles a la versió comercial. El suport de la comunitat i dels desenvolupadors per a la versió gratuïta és minsa. Per l'altre, el sistema es nodreix de NAGIOS per a la monitorització, i en si és un sistema molt complet de gestió d'incidències.

5.2.5.3 Conclusions

Donat que en quan a monitorització, Zenoss ens ha convençut molt més que NAGIOS, i no necessitem un sistema de *ticketing* en aquest moment, hem descartat OSSIM com un component de la nostra arquitectura.

5.2.6 Conclusions

Podríem classificar els diferents sistemes d'informació que hem provat en tres categories: sistemes de monitorització (NAGIOS, Zenoss), SIEM (*Security Information and Event Management* – OSSIM) i Toolkits (NST).

Pel que fa als dos sistemes de monitorització estudiats, Zenoss ha estat l'escollit per la seves prestacions i senzillesa en front a NAGIOS. Les seves capacitats d'operació via web son totals, de tal manera que durant les proves mai hem hagut d'obrir un terminal, mentre que amb NAGIOS constantment s'està operant i editant configuracions a través de consola, el que obliga a uns que els operadors disposin d'uns coneixements més elevats.

Tot i que un dels nostres objectius era la implementació d'un sistema de correlació d'esdeveniments, el que ens va fer avaluar un SIEM, la realitat de la implementació d'un sistema d'aquest tipus en una xarxa com la analitzada supera l'envergadura d'aquest TFC. Això, i un cop descobertes les funcionalitats de correlació de Zenoss, és el que ha motivat la utilització d'un arquitectura composada per un sistema de monitorització i un *toolkit*.

5.2.7 Disseny de l'arquitectura

La nostra arquitectura estarà composada per NST i Zenoss. De manera independent, tenim instal·lat inSSIDer en un parell de portàtils que ens serveixen per fer mesures de camp.

Cada un d'aquests components (NST i Zenoss) funcionarà en una màquina virtual, de les quals hem fet diversos *snapshots* en diversos moments de la seva instal·lació el que ens permet tornar a un estat anterior amb molta rapidesa i facilitat. Ambdós sistemes són administrables i operables des de web, el que permet desplegar-los a l'entorn d'operacions amb molta facilitat i certa independència de les seves dimensions. S'ha creat a Zenoss un compte d'administració, que permet editar els dispositius, i diversos d'operació, que permet als operadors explotar el sistema que han configurat els administradors.

En la arquitectura de sistemes d'informació que hem desplegat, Zenoss aporta la monitorització sobre els dispositius i genera les alertes corresponents, alhora que centralitza els *logs* dels dispositius. NST en canvi, s'utilitza sota demanda d'un operador que necessita fer ús d'una de les eines del *toolkit* per atendre una incidència en el servei. Una excepció a això és SNORT, un dels components de NST que pot executar-se sota petició està sempre actiu i que realitza funcions de detecció d'intrusions.

Zenoss	NST
Correlació de successos	
Alertes	Detecció d'anomalies
Monitorització	Eines centralitzades
Centralització de logs	

Taula 5.1 Components de l'arquitectura

Un operador dels sistemes ha d'atendre dues finestres: les alertes que mostra zenoss a través de la seva interfície i les que mostra BASE (un *frontend* d'SNORT) en la seva. Si es necessari utilitzar NST, es pot fer en un navegador en qualsevol de les dues pantalles.

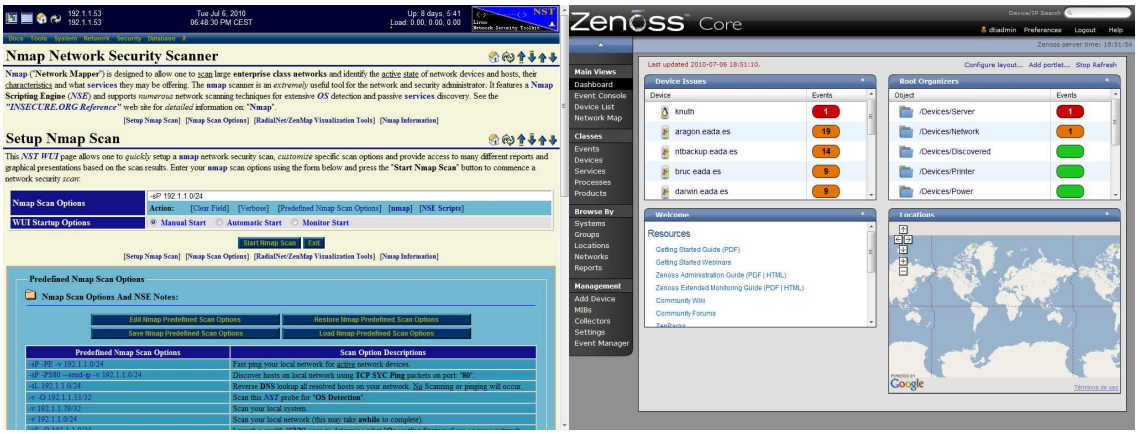

Fig. 5.7 Entorn d'operacions amb dues pantalles

6. CAPÍTOL 6. IMPLEMENTACIÓ

Un cop escollides les eines i els sistemes d'informació, en aquest capítol es detallen, en primer lloc, les correccions tècniques sobre la xarxa WiFi i, en segon lloc, el desplegament dels sistemes d'informació i la seva configuració per a interactuar amb els diversos dispositius de xarxa.

6.1 Mesures a curt termini: correccions en la xarxa WiFi

Partint dels resultats de l'anàlisi efectuat, en aquest apartat s'efectuen correccions tècniques sobre la xarxa WiFi.

6.1.7.1 Canvi contrasenyes APs

S'han configurat diferents contrasenyes per cada AP, de major fortalesa que les existents. Hem utilitzat contrasenyes de 8 caràcters combinant aleatòriament mitjançant un generador números y caràcters especials. Alguns d'aquests caràcters especials provocaven que l'accés als AP fos impossible un cop configurades, possiblement per algun problema relacionat amb el joc de caràcters. Hem detectat els caràcters problemàtics i els hem substituït per caràcters alfabètics.

6.1.7.2 Substitució APs

Donades les lectures de l'anàlisi de tràfic, es canvien aquells punts d'accés que generen un tràfic corrupte. En una segona etapa, es procedirà a canviar la resta per aprofitar les noves característiques i, donat que en aquestes correccions es desenvolupen en paral·lel el desenvolupament dels sistemes d'informació, treure profit de les millors capacitats de monitorització.

El nou model d'AP és de classe empresarial i disposa de noves característiques:

Disseny més adient:
- suport mural assegurable amb cadenat
- xassís de metall més resistent

Prestacions (s'han implementat totes):
- PoE: permet prescindir de l'alimentació, el que ens dóna mes flexibilitat en la ubicació de l'AP i ens permet assegurar aquells APs que estaven connectats a un endoll a l'abast dels usuaris. També permet el reinici en fred del *hardware* remotament, ideal per aquells APs instal·lats en ubicacions de difícil accés i per estalviar desplaçaments.
- Majors capacitats de monitorització remota: SNMP v2

- Més opcions de securització:
    - o accés per SSH
    - o filtre que permet impedir l'accés de la gestió per WLAN

6.1.7.3 Remapeig de canals

S'optimitza l'ús del espectre lliure utilitzant canals amb menys ús i de tal manera que dos BSS de la nostra xarxa no es solapin. Per tal de poder-ho controlar, es desactiva la característica de canal dinàmic i es defineix el canal de cada AP tenint en compte la seva ubicació respecte als demés. L'eina *inSSIDer* ens permet veure visualment la utilització dels canals 802.11 a la banda de 2.4 Ghz.

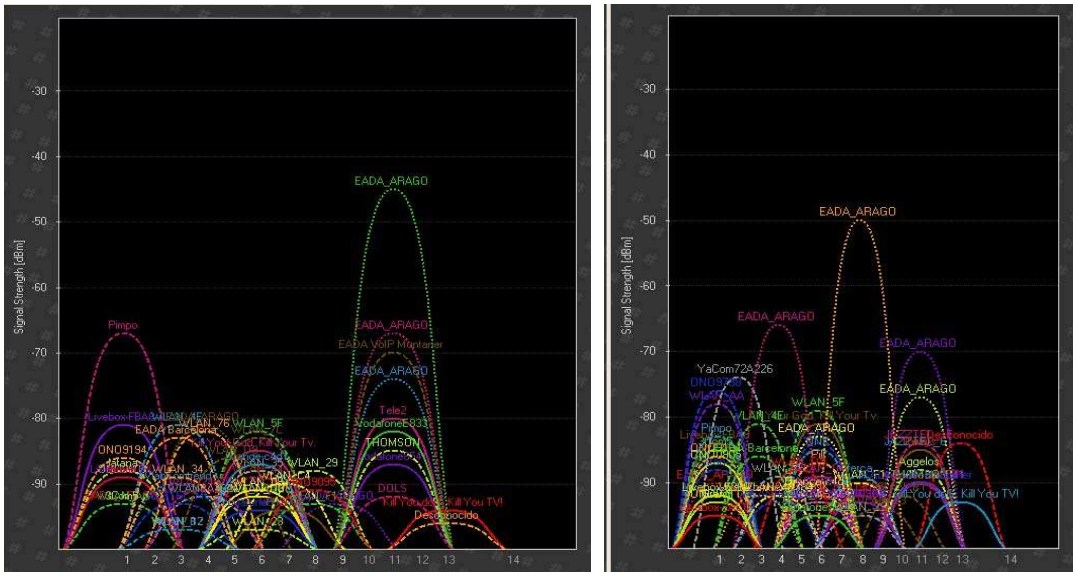

Figura 6.1 Optimització de canals ràdio

6.1.7.4 Retirada de 3 antenes Yagi (Contenció de cobertura).

4 del punts d'accés tenien connectada una antena Yagi. Es comprova fent un mapeig de la cobertura amb inSSIDer que, per la zona a la que volem donar cobertura, l'ús d'aquesta antena no és adequat en 3 APs. Amb aquesta acció hem contingut la cobertura als límits de l'edifici, el que ens protegeix contra atacs de l'exterior.

6.1.7.5 Reorientació d'una Antena Yagi i eliminació d'un AP (Contenció de cobertura).

Es readjusta la orientació de l'antena de tal manera que podem donar cobertura a una zona més extensa, el que ens permet retirar un AP.

6.1.7.6 Xifrat de la xarxa

Un cop avaluades les característiques del servei que dóna la xarxa, s'ha escollit un xifrat *WPA-PSK*. Tot i conèixer que aquest xifrat no és totalment segur, la tria ha vingut condicionada per les necessitats d'una ràpida implementació amb els recursos disponibles (es pot implementar sense haver de desplegar servidors *RADIUS*) i d'haver de garantir a l'usuari la compatibilitat amb estacions i dispositius *legacy*.

Com que es coneixen les limitacions i vulnerabilitats d'aquest tipus de xifrat, s'ha triat una contrasenya de 26 caràcters alfanumèrics, i se'n ha recomanat al departament el canvi periòdic.

Amb aquesta acció s'estableix un control d'accés que permet acotar el servei ofert només a aquells usuaris autoritzats, reduint de forma notable la càrrega sobre la xarxa.

6.1.7.7 Desactivació WMM

Donat que la priorització de tràfic no és necessària a la xarxa, desactivem les extensions multimèdia (WMM, *Wireless MultiMedia*) per tal de reduir el risc d'atacs que aprofiten les vulnerabilitats QoS WPA conegudes.

6.2 Mesures a llarg termini: implementació de sistemes d'informació

En aquest capítol es recull la implementació dels sistemes d'informació a l'entorn d'operacions. Donat que NST funciona com una suite d'eines sota demanda (escaneigos, *sniffing*) no necessita adaptar-se, amb la excepció d'Snort.

6.2.8 Adaptació d'Snort

Per tal de que Snort pugui capturar dades correctament, necessita fer-ho directament del medi físic de transmissió. Donat que l'entorn Ethernet és commutat, això obliga a la inserció d'un hub en el tram que volem estudiar o a la configuració d'un port de *monitoring* o *mirroring* en els switchos.

6.2.9 Integració Snort en Zenoss

Per tal d'arribar al màxim nivell de centralització de monitorització, hem provat d'integrar els missatges de Snort dintre de NST en Zenoss. Es prova la

instal·lació d'un syslog-ng en la màquina NST que redirigeixi els logs al Zenoss, però els missatges no arriben en un format intel·ligible. Donat que NST forma part del nostre disseny i aquest conté una bona explotació de les dades d'SNORT amb BASE, SNORTER i SnortSlinger, hem decidit que la monitorització de la detecció d'intrusions que realitza SNORT es farà a través de NST, donat que el nostre entorn d'operacions ja hi dedica una pantalla.

6.2.10 Configuració dels dispositius a Zenoss

6.2.10.1 Monitorització de Rendiment:

Per a obtenir les gràfiques de rendiment dels diferents dispositius del sistema, hem avaluat les següents tècniques:

- SNMP a través d'un zenPack
- SNMP a través de SNMPInformant, un *plugin* SNMP que s'instal·la al dispositiu
- SNMP a través d'agents propis del fabricant del *hardware*
- WMI per a servidors Windows.

La tercera opció és la que ofereix una millor profunditat de les dades que s'obtenen. Per exemple, en servidors HP Proliant es poden observar els diferents ventiladors del sistema.

De les altres tres, és a dir, en aquells casos en que no disposem d'agents SNMP propis del fabricant, WMI és la més convenient per la seva facilitat, major profunditat, seguretat, i la no necessitat de instal·lació ni tan sols del servei SNMP al sistema remot.

6.2.10.2 Monitorització per WMI:

Un cop instal·lat el *zenPack* de monitorització de rendiment WMI, a l'objecte:

1) Cal introduir les dades d'un compte del sistema que tingui permisos per utilitzar WMI a les *zProperties*.
2) Cal afegir els *plugins* que ha creat el *zenpack* a *zCollectorPlugins* per sobre del *plugins* zenoss.snmp, o esborrar aquests. Hem decidit deixar-los ja que d'aquesta manera també es recopila informació a través de SNMP (si el dispositiu està convenientment configurat, en cas contrari, o si el dispositiu no serveix SNMP, cal esborrar aquests i situar la *zProperty zSNMPMonitorIgnore* a *True*).
3) A *templates*, cal fer un *binding* amb la la plantilla WMIDevice per tal de que les dades de rendiment s'obtinguin per WMI
4) Si es desitja obtenir els canvis immediatament, es pot llençar un remodelament del dispositiu.

6.2.10.3 Centralització de logs:

Un dels inputs d'informació del sistema Zenoss es el syslog integrat, que permet configurar tota mena de dispositius perquè n'enviïn els seus logs de manera molt senzilla. D'aquesta manera, podem aprofitar les funcionalitats de deduplicació per als logs, i tenir un únic lloc per tots els logs, el que facilita enormement la seva posterior correlació.

6.2.10.4 Monitorització per SNMP:

Per aquells dispositius que no siguin Windows o tot i ser-ho no pertanyin a un domini (en aquest cas la configuració és excessivament complicada i per tant WMI perd avantatges davant de SNMP) es configura la monitorització per SNMP, que en Zenoss és totalment nativa. Tot i la seva inseguretat, hem utilitzat en alguns casos SNMPv2 per ser aquesta versió la màxima suportada pels dispositius. Allà on ha estat possible, hem configurat l'enviament de *traps* SNMP a la màquina Zenoss, on es recullen també de manera nativa.

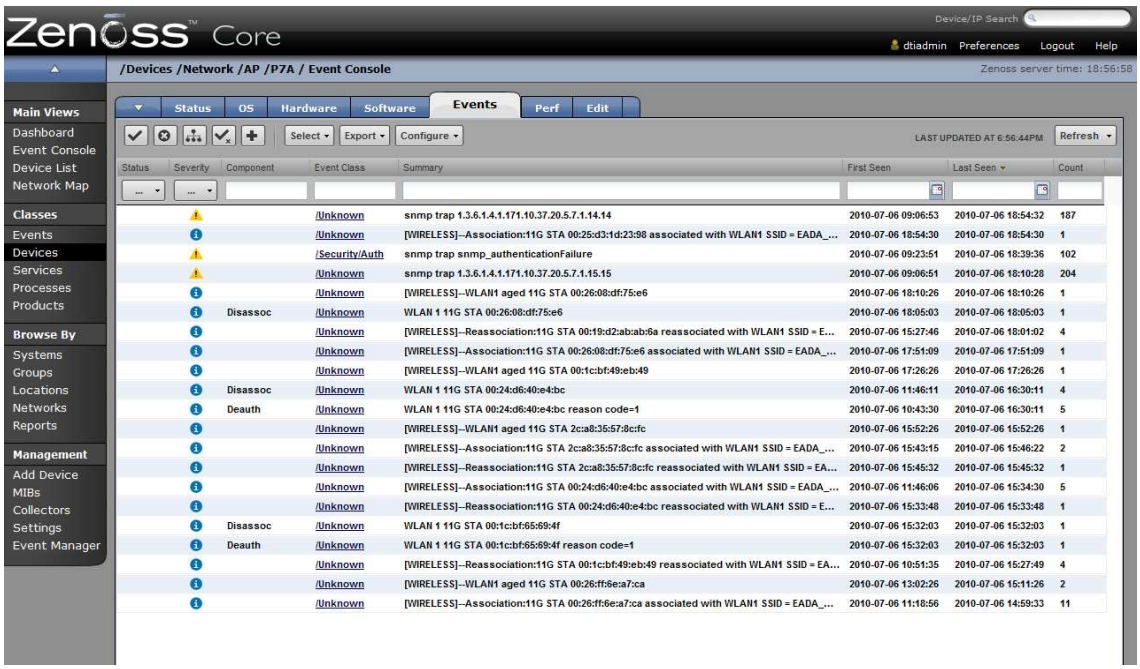

Figura 6.2 Esdeveniments d'un AP monitoritzat per SNMP, on es poden apreciar els traps

6.2.10.5 Propietats i classes

Volem incorporar a Zenoss diversos equips de sobretaula que donen servei als estudiants i a les aules de la institució. Hem escollit WMI pels motius exposats. Donat que aquests equips estan agrupats sota diferents credencials d'administració, creem una sèrie d'organitzadors dintre d'una nova classe /desktop/Nom. Aquests organitzadors permeten definir *zProperties* per cada un

d'ells, de tal manera que afegint els equips directament al corresponent organitzador n'heretaran la configuració. En les *zProperties* es defineixen les credencials d'accés al sistema a monitoritzar, així com quins plugins de recol·lecció d'informació utilitzarà el zenoss, i quina font utilitzarà per a elaborar les gràfiques de rendiment. Les *zProperties* segueixen un esquema d'heretament de les classes superiors, el que simplifica molt la configuració de múltiples dispositius similars. Per exemple, per configurar les credencials remotes d'accés (compte WMI o *communities* SNMP), aquestes es poden un introduir un sol cop en la classe que conté els dispositius.

6.3 Resultats i conclusions

La introducció de Zenoss en el departament de tecnologies de la informació ha permès, en primer lloc, un canvi substancial en la visió dels equips importants a la xarxa. S'ha eliminat l'anterior situació de ceguera en que cap sistema mostrava l'estat dels diferents dispositius i per tant es reaccionava a les incidències quan es percebien, el que no garantia una bona continuïtat del servei, donat que no existeix una línia directa de comunicació d'incidències entre l'usuari final de la xarxa WiFi i el departament. Gràcies a la monitorització de Zenoss i tal com es mostra en la figura inferior, una sola pantalla accessible per qualsevol operador mostra visualment l'estat de tots els equips de xarxa, amb un codi de colors jeràrquic que indica la gravetat i el nombre d'esdeveniments actuals del dispositiu no processats pels operadors.

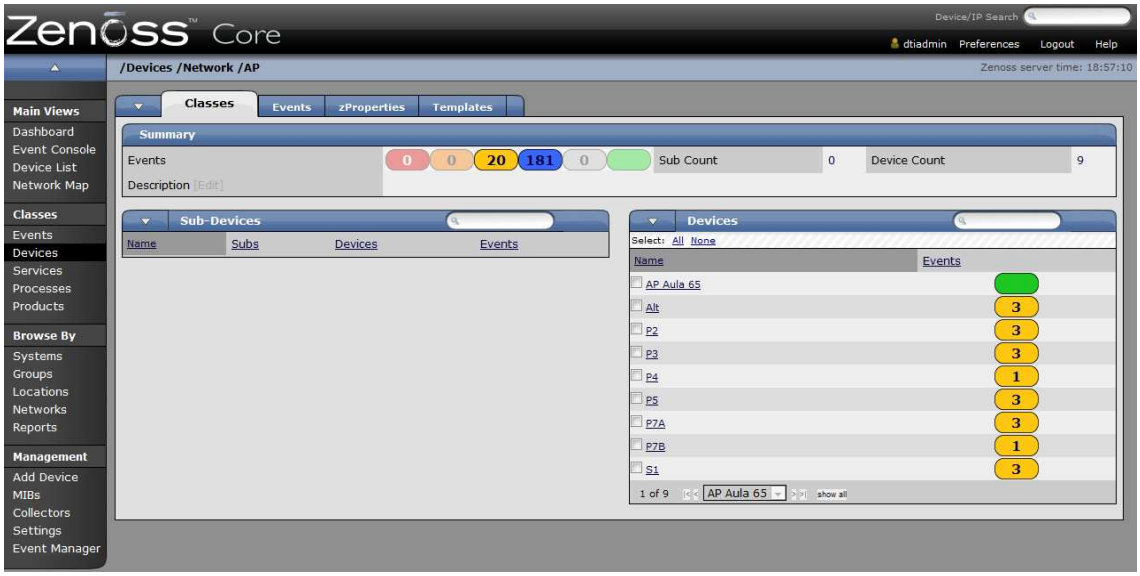

Figura 6.3 Estat dels APs dintre de la classe /Network

En segon lloc, la informació continguda a Zenoss és un registre de l'activitat del dispositiu obtinguda gràcies a la monitorització permanent. Això permet

diverses accions, com l'avaluació del rendiment i del dimensionament d'equips i enllaços en un moment puntual o al llarg del temps (figura 6.4), i és de gran utilitat en l'anàlisi forense de fallades dels sistemes.

Figura 6.4 Gràfiques de rendiment temporals d'un AP

En tercer lloc, la organització dels dispositius de la base de dades de Zenoss en la seva interfície permet navegar-hi com si d'una base de dades de configuració (CMDB, *configuration management database*) o d'inventari es tractés. Això permet accedir quan és necessari a consultar qualsevol aspecte de la configuració d'un dispositiu de manera ràpida, actualitzada i centralitzada. A la figura 6.5 es poden veure en una sola pantalla les adreces MAC i IP de les interfícies del dispositiu, així com les rutes IP establertes.

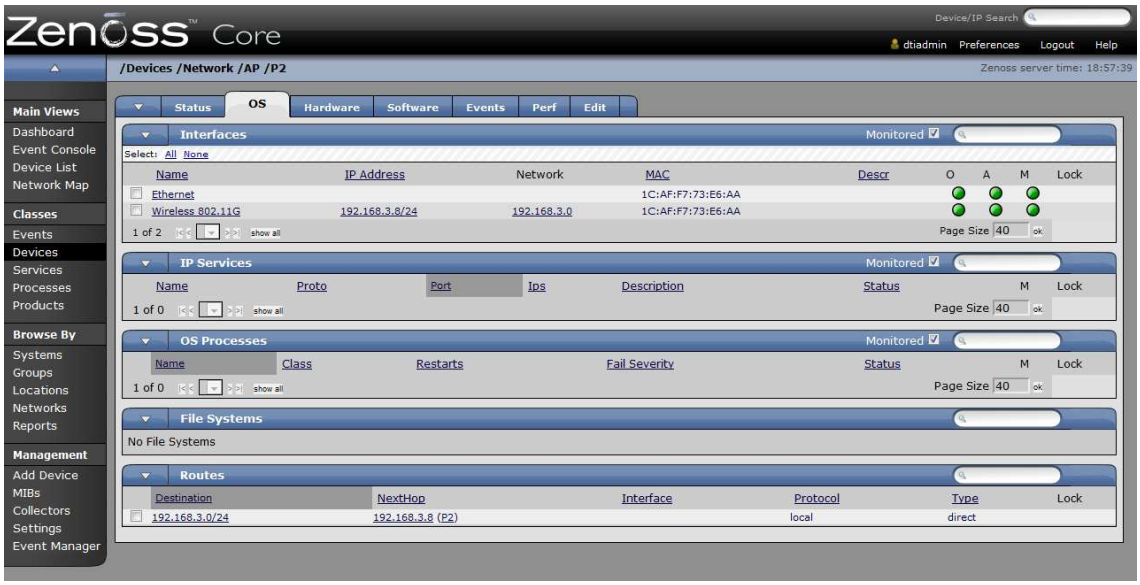

Figura 6.5 Configuració de xarxa a nivell SO d'un AP

Després de la execució de les correccions sobre la xarxa WiFi hem començat a observar mitjançant els sistemes d'informació quin és el servei real a l'usuari que dóna la xarxa WiFi. Tot i que el temps de servei és major, i la resposta a incidències és molt més ràpida i precisa que abans, hem observat que en situacions puntuals on la càrrega de trànsit és molt elevada, es produeixen fallades intermitents del servei de connexió a Internet. Fent proves quan aquesta situació es produïa, hem detectat que el servei de DNS falla en produir-se un *timeout* en les peticions de resolució. Les característiques d'aquest trànsit (missatges molt curts i freqüents que contenen una gran proporció de capçaleres en relació al missatge DNS, i que habitualment s'envien per UDP) fan que aquest trànsit sigui especialment vulnerable a fallar en condicions de molta càrrega als enllaços troncals.

Aquestes dades ens han portat a cercar una millora en la robustesa del servei en condicions extremes, havent resolt en la modificació del *gateway* de la xarxa WiFi per tal d'incloure-hi un *proxy* transparent, que incorpora una memòria cau de peticions HTTP que alleugera els troncals de connexió a Internet, alhora que proporciona un mecanisme de seguretat en no enrutar cap tipus de tràfic i només servir peticions HTTP.

Una de les limitacions més importants en aquests sistemes (concretament s'està treballat amb Squid3 i iptables sobre una base d'Ubuntu Server 10.04) és que no poden servir tràfic HTTPS, per la manera com aquest combat els atacs *man-in-the-middle*, pel que aquest tràfic s'ha d'enrutar a través de la màquina en la que corre el *proxy*.

Pel que fa al servei de DNS necessari per a la navegació web, que o bé s'enruta com es fa amb l'HTTPS, o bé s'implementa a la xarxa o en el mateix servidor en forma d'un servidor DNS. Aquesta opció ha estat la triada per la

conseqüent millora en el rendiment global de la xarxa en proveir una memòria cau de DNS, pel que s'ha implementat BIND9 com a reenviador en el mateix servidor.

Pel que fa al servei DHCP, necessari per a l'adreçament automàtic de les estacions, ha de servir-se des de la pròpia xarxa (o des del mateix servidor intermediari com s'ha fet en el nostre cas) i establir el servidor *proxy* com a *gateway* de les estacions, qui intercepta les peticions y les tracta com a *proxy* i no com a enrutador (es per això que aquest tipus de *proxy* s'anomena també interceptor).

Aquest servidor és transparent per les estacions, que es comuniquen amb ell a nivell IP com si es tractés d'un enrutador més. Això elimina la necessitat de la configuració dels clients i permet un desplegament del servidor sense actuacions a les màquines dels usuaris.

7. CAPITOL 7. BALANÇOS

7.1 Generals

Aquest treball hereta gran part de la base teòrica del desenvolupament d'un primer TFC (inacabat) en el que l'autor treballava anteriorment que tenia per objectiu el desenvolupament d'un *toolkit* per a auditar xarxes WiFi, que seria utilitzat en l'anàlisi de la xarxa que aquest TFC analitza i que va ser replantejat quan la meva dedicació laboral en el client va augmentar. El fet d'haver treballat en seguretat WiFi abans de començar l'actual TFC ha permès definir uns objectius realistes i acotats, i una planificació molt més encertada, quelcom que no varem aconseguir en l'anterior TFC. Tot i la pèrdua d'hores de feina que el canvi de TFC va suposar, la experiència de l'anterior ha permès que aquest sigui un TFC més realista pel que fa a la valoració inicial.

7.2 Valoració de l'acompliment dels objectius

O1. *Ampliar la formació sobre la seguretat WiFi per tal d'obtenir els coneixements que constitueixin una base teòrica.*

En aquest treball s'ha aprofundit molt sobre la seguretat WiFi. A mesura que s'anava avançant en l'estudi, és feia palesa que l'extensió i profunditat en aquest tema vindrien limitats per la extensió de la memòria d'aquest TFC. Així doncs, s'ha fet necessari seleccionar els continguts que apareixen en els capítols 2 i 3. Lamento no haver pogut incloure molts més continguts que he après durant la cerca i triatge d'informació, i que considero que també poden constituir una bona base teòrica per aquest TFC i un bon manual de referència pel Departament. Entre aquests continguts s'inclouen la descripció d'aquelles tècniques d'atacs, que si bé no totes són pròpies de la tecnologia (motiu per al qual han estat les triades a no aparèixer per tal de mantenir una llargada adequada) son d'aplicació a WiFi. Estic parlant de tècniques com *Man In The Middle, Evil Twin* o *Rogue AP*, que són de les més perilloses pel que fa a risc de captura no autoritzada d'informació i que sovint s'utilitzen per a explotar vulnerabilitats que si s'han inclòs.

O2. *Aprendre conceptes bàsics d'auditoria tècnica de seguretat, per tal de poder abordar l'anàlisi de la xarxa en qüestió des d'aquesta perspectiva.*

L'estudi dels continguts d'aquest objectiu ha permès una anàlisi tècnica de la xarxa problemàtica molt més procedimentat i rigorós que si aquest no s'hagués inclòs, tot i que això és poc visible a la memòria escrita. Tal i com s'indica al capítol 2, l'auditoria en tàndem aplicada a la xarxa WiFi que s'ha estudiat en aquest treball comprova rigorosament l'objectiu, però no proporciona informació sobre la resposta d'aquest davant variables inesperades. De poder aconseguir això últim, en el context en el que ens trobem hagués resultat inútil, ja que el

departament no disposava d'eines, mesures ni procediments per a respondre a incidències.

O3. *Cercar, avaluar i seleccionar les eines de treball apropiades.*

Com ja s'ha mencionat anteriorment amb les tasques respectives a aquest objectiu, aquest s'ha desenvolupat en paral·lel a la resta. Això ha estat així degut a la enorme quantitat d'eines i distribucions Linux disponibles per a la seguretat WiFi, el que ens ha permès triar el què necessitàvem. He trobat eines molt interessants, que han passat a formar part del meu *toolkit* personal i que utilitzo amb freqüència. Aquelles eines i en especial els sistemes d'informació que finalment s'han implementat en el client compleixen sobradament els objectius marcats, amb la excepció parcial del sistema de correlació d'esdeveniments, tal i com s'explica més endavant.

O4. *Analitzar la xarxa WiFi objecte d'estudi.*

L'anàlisi efectuat sobre la xarxa WiFi ha donat suficient informació per a realitzar aquest TFC i dibuixar algunes accions futures. Les deficiències que s'han identificat com a resultat han permès efectuar unes correccions que han tingut un impacte real sobre el servei de la xarxa. És per això que es pot concloure que ha estat un bon anàlisi. Si bé acadèmicament i tècnica se'n pot realitzar un de més extens i profund, desde la perpectiva empresarial s'ha obtingut un bon ratio cost-benefici, obtenint resultats significatius amb eines de cost zero i una dedicació de recursos humans acotada.

O5. *Transmetre una base de coneixement de la tecnologia al departament de TI del centre aplicada a la seva xarxa WiFi i orientada a millorar el servei.*

Durant la execució de les fases finals d'aquest treball, s'han realitzat sessions informatives i formatives a membres del departament de TI. S'han redactat diversos documents que plasmen l'anàlisi i la motivació i descripció dels canvis que s'han realitzat a la xarxa. També s'han elaborat manuals d'operacions d'aquells sistemes d'informació (Zenoss) que poden ser operats per diversos perfils dintre del departament. Així mateix, s'han elaborat procediments de resposta a incidències amb diagrames de flux per donar resposta immediata a alteracions del servei.

O6. *Dissenyar i executar la implementació de mesures correctives sobre la xarxa que permetin augmentar la disponibilitat de la xarxa i minimitzar el temps d'aturada.*

> O6.1 *Augment de la disponibilitat (uptime o temps de servei) a través d'incrementar la seguretat i dissenyar i executar aquelles millores tècniques que s'estimin adients.*
>
> S'ha aconseguit una millora real de la disponibilitat en la xarxa WiFi. Les millores tècniques realitzades han permès que el servei sigui continu i sense aturades sense motiu conegut (e.g. fallades elèctriques). Els canvis tècnics introduïts han permès eliminar tràfic indesitjable que era generat per equips

desfasats, en ésser aquests substituïts per uns de nous més estables i que no es saturen en moments de pic de molts usuaris. Això ha suposat un canal més net i que per tant, rendeix més.

O6.2 *Minimització del temps d'aturada (downtime o interrupció del servei). Això s'ha aconseguirà a través de:*

1. *Augment de la capacitat de resposta davant d'incidències i caigudes de serveis. Per tal de aconseguir-lo és dotarà de més coneixement i més eines al departament.*

   El coneixement d'eines s'ha transferit a altres membres del departament, el que ha millorat la seva preparació. Eines com inSSIDer són utilitzades en la resolució d'incidències i en el manteniment dels APs. Es coneix la importància d'una bona distribució del canals ràdio, així com de la contenció de cobertura. Els membres del departament han pogut veure com la utilització de *hardware* i eines professionals ha permès solucionar la situació anterior a aquest TFC.

   Per altra banda, s'ha redactat documentació d'operacions en Zenoss, per poder estendre el coneixement a tots els membres del departament, pels quals ha estat creat un compte individual a l'eina. També s'han documentat mapes de xarxa i procediments per a la instal·lació i el manteniment del *hardware*.

2. *Desplegament de sistemes de monitorització i alertes que permetin conèixer més ràpidament i profunda els esdeveniments dels sistemes.*

   Com a conseqüència de la implementació de Zenoss, existeix coneixement de l'estat de la xarxa en tot moment al departament, el que tal i com volíem es tradueix en un menor temps de resposta i resolució més ràpida d'incidències. En el temps que aquesta eina porta funcionant, s'han detectat instantàniament aquells casos en que el hardware ha deixat de funcionar o s'ha perdut connectivitat per una causa coneguda (e.g. fallada elèctrica o un manteniment del cablejat).

3. *Implementació d'un sistema de correlació d'esdeveniments que ens ajudi en l'anàlisi de situacions.*

   Aquest objectiu es va incloure per tal de disposar d'un sistema que permetés l'anàlisi a posteriori d'esdeveniments, que ajudés en la resolució d'incidències i la millora dels sistemes. Lamentablement, el *software* que incorporava aquesta funció (OSSIM) va ser descartat per la seva grandària i feixuguesa. Zenoss aporta algunes característiques en aquesta línia, i, si bé no es pot considerar un veritable sistema de correlació d'esdeveniments, el departament i la seva direcció estan satisfets amb el que Zenoss aporta en aquests casos, ja que la centralització dels logs dels sistemes i la

deduplicació permet una eventual correlació manual d'una manera molt lleugera.

O7. *Valorar les millores efectuades i proposar línies futures d'actuació.*

Finalment a les conclusions finals del treball es valoren amb detall les millores efectuades. Amb la realització d'aquest TFC s'han obert múltiples línies futures d'actuació que es detallen més endavant.

7.2.1 Altres objectius assolits.

O8. Una de les aplicacions dels sistemes d'informació instal·lats ha estat implementar un *core* (nucli) comú a les diverses xarxes que té la institució. Actualment es continua treballant en aquest línia. El servidor on s'executa Zenoss té diverses interfícies que permeten connectar-lo a les diverses xarxes.

O9. S'ha configurat el Zenoss perquè aquest enviï alertes per correu electrònic quan es produeixen esdeveniments crítics com la caiguda d'un servei o dispositiu.

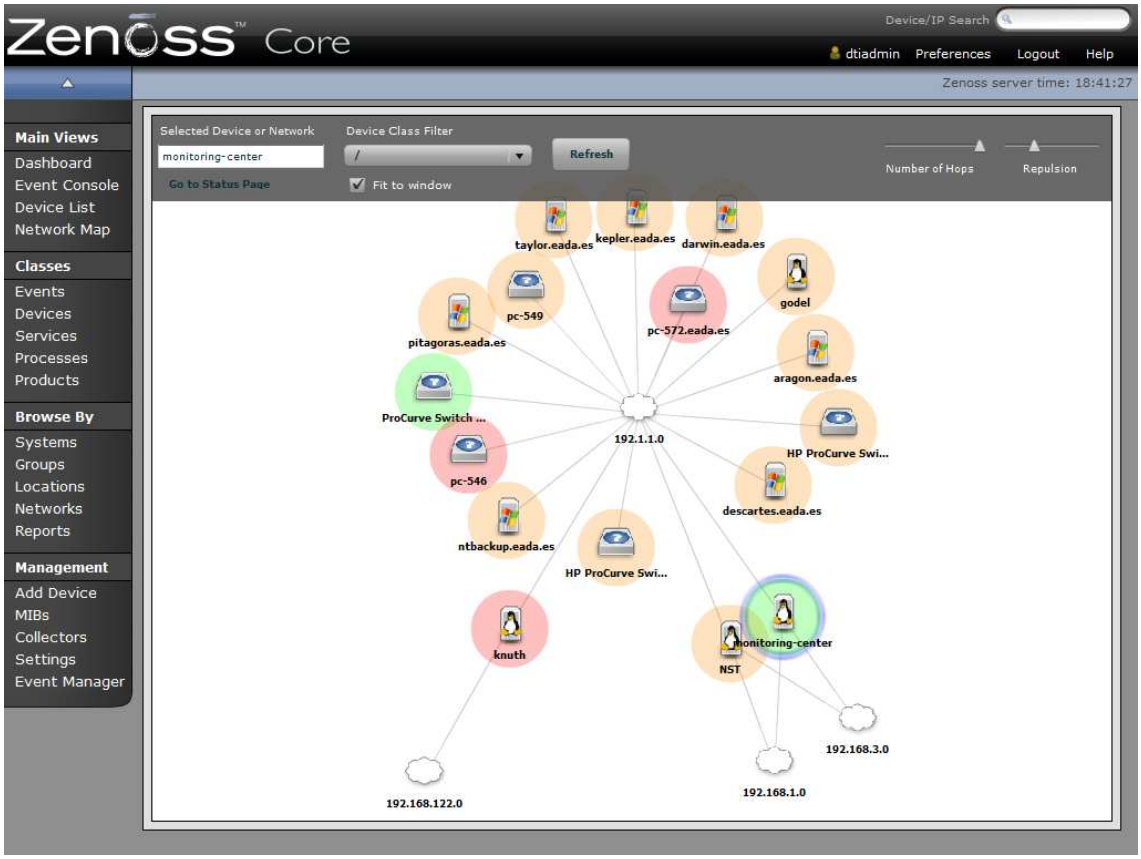

Figura 7.1 *core* de sistemes d'informació connectat a diverses xarxes

O10. La introducció d'un servidor cau intermediari transparent ha augmentat considerablement el rendiment del servei, optimitzant la utilització de l'ample de banda del troncal de connexió a Internet.

7.3 Valoració de l'acompliment de la planificació i els costos

La planificació del TFC ha patit una desviació respecte a les previsions inicials. En primer lloc, tot i que la redacció de la memòria es va incloure implícitament en la planificació donat que aquesta s'ha redactat a mesura que s'anava avançant, no és va planificar la composició de format d'aquesta com una tasca, el que ha provocat que la planificació quedés curta. Altres factors han estat, com ja s'ha exposat a les conclusions del capítol 3, l'extensiu volum d'informació trobada sobre seguretat WiFi que ha obligat a realitzar una cerca més llarga i un triatge no planificats.

D'altra banda, tasques que durant la planificació semblaven més propenses a patir una major variació de dedicació, com la instal·lació dels sistemes d'informació, han resultat acurades en la seva valoració i fins i tot (com en el cas de la posada en funcionament de Zenoss a partir del instal·lador *stack*) s'han realitzat en menor temps del previst.

Finalment, la extensió dels sistemes d'informació a totes les xarxes de la institució (especialment pel que fa a Zenoss) per una banda, i la introducció del *proxy* transparent com a porta d'enllaç per l'altre, ha causat una desviació important en la planificació en no ser, aquestes actuacions, contemplades inicialment. S'ha optat per incloure-les, en considerar per una banda l'extensió dels sistemes molt profitosa, i per l'altre la implementació del *proxy* necessària per a l'acompliment dels objectius, quan, un cop efectuades les correccions a curt termini sobre la xarxa WiFi, es va constatar gràcies als sistemes d'informació la saturació dels troncals en condicions normals d'ús.

Els costos en aquest treball han estat únicament de hores de feina. Pels motius esmentats, els costos reals han superat els previstos, en realitzar-se algunes hores més de les planificades.

A la finalització del TFC, s'han realitzat 40 hores més de les previstes, el que condueix al següent excés de treball:

$$\text{Desfasament} = \text{Hores excés} / \text{Hores totals} = 40\ \text{h} / 272\ \text{h} = 14{,}7\ \%$$

7.4 Línies futures

- Millora del xifrat:

  De les vulnerabilitats del xifrat WPA-PSK que s'ha hagut d'implantar a la xarxa, no s'han pogut establir contramesures per a l'atac intra-psk descrit a 3.2.3.1. Això conjuntament amb la voluntat d'establir un millor sistema d'autenticació basat en usuaris, indueix a la propera implementació de WPA-Enterprise o a la reconsideració de WPA2-Enterprise.

- Portal captiu:

  Relacionat amb el sistema d'autenticació, resulta interessant la futura implementació d'una solució de portal captiu que permeti un accés a la xarxa més lleuger i segur als usuaris.

- Integració de Zenoss amb sistemes de *ticketing*:

  La necessitat del departament per a disposar d'un sistema de *ticketing* propi per a la gestió d'incidències, obre la possibilitat d'integrar els nostres sistemes d'informació amb aquest futur sistema. En aquesta línia, hem trobat documentació sobre la integració de Zenoss amb Remedy, tot i que l'elevat cost d'aquesta solució fa previsible la decisió d'utilitzar un altre *software*. En aquest cas, si la comunitat Zenoss no proveeix de ZenPacks per a la integració, s'haurà de treballar en el desenvolupament.

- Millora del sistema de correlació d'esdeveniments:

  Un dels objectius del TFC era la implementació d'un sistema de correlació d'esdeveniments. Aquest objectiu no s'ha assolit totalment, el que obre la possibilitat del seu desenvolupament futur.

8. CAPÍTOL 8. CONCLUSIONS

8.1 Generals

L'elevat nombre d'objectius assolits s'ha traduït en una millora real en la qualitat del servei ofert als usuaris a través de la xarxa WiFi. Les millores s'han produït en estabilitat, en temps de servei, en rendiment, i en seguretat.

Els beneficis per a la empresa han estat diversos, destacant un major *uptime* i un menor número d'incidències amb els mateixos recursos. Per altra banda, el coneixement obtingut amb aquest treball realitzat a la xarxa WiFi es pot exportar a les altres xarxes de la empresa. Actualment, els sistemes d'informació s'estan integrant en altres xarxes que contenen els serveis informàtics crítics de la institució.

Durant l'anàlisi de la xarxa WiFi, moment en que aquest TFC entrava en contacte amb el cas real, van començar a sorgir les diferències entre el món de l'empresa i l'acadèmic. En primer lloc la interacció del desenvolupament del treball amb el món real d'un servei viu en una empresa, ha causat que es generessin nous *inputs* d'informació a mesura que s'anava avançant, el que ha causat, com en el cas de la decisió d'incorporar un servidor cau intermediari transparent al final del treball, una desviació important de la planificació inicial.

Per altra banda, el TFC s'ha construït amb una forta base teòrica, per tal de fonamentar un anàlisi rigorós des del punt de vista acadèmic. És en el moment d'aplicar la teoria quan l'anàlisi de costos i beneficis decideix quines accions son apropiades o no, pel que moltes accions que tenien un gran interès acadèmic (estudis de la utilització de l'espai radioelèctric, desplegament d'una estructura de sensors de WIDS (*Wireless Intrusion Detection Service,...*) no s'han realitzat perquè els seus costos d'equipament i hores de feina no justificaven el benefici que aportaven.

És interessant incorporar a la mentalitat d'un enginyer a punt de finalitzar els estudis, que en el món empresarial són els resultats ponderats per aquest balanç cost-benefici els que dirigeixen les estratègies tècniques per assolir un objectiu. Això introdueix un concepte no vist a la carrera, el del risc. Potser una solució implementada no és la millor des del punt de vista tècnic, però és suficientment bona tenint en compte el risc que té de fallada si és valora el cost d'una de millor. Una bona mostra d'això és la utilització d'un xifrat menys segur que una altra disponible en la xarxa WiFi que s'ha estudiat, per tal de poder mantenir un servei menys restrictiu amb els requisits dels usuaris.

Tot i que una situació com aquesta genera certa incomprensió i decepció en no poder resoldre un problema donat (tal i com se'ns ensenya a la carrera) de la millor manera possible, trobo que també és més humana perquè hom és pregunta "a costa de què?", té en compte més variables que les purament tècniques (en aquest cas un servei més còmode a una minoria d'usuaris) i ens recorda que no tot és possible sempre. En qualsevol cas, aquesta és la manera

d'adaptar la enginyeria a la realitat, i cal adonar-se'n d'això en el moment de redactar les últimes línies d'un treball que conclou uns estudis universitaris.

8.2 Ambientalització

Aquest TFC ha tingut en compte un factor ambiental molt important amb la contenció de senyal dins dels límits de l'edifici. En l'estudi inicial de la xarxa WiFi, varem constatar la contaminació radioelèctrica en la banda dels 2.4 Ghz existent.

Per tal de poder obtenir una bona SNR respecte al soroll composat per totes les xarxes WiFi veïnes (i demés aparells domèstics o d'oficina que operen en la banda) havíem de transmetre amb més potència o col·locar mes APs del que hagués estat necessari amb una banda de 2.4 Ghz neta d'interferències.

La decisió de contenir la cobertura de la nostra radiació 802.11, també motivada per motius de seguretat, contribueix a no embrutar l'espai radioelèctric del veïns.

Aquest TFC, per altra banda, no ha presentat un impacte mediambiental mesurable en el seu desenvolupament.

8.3 Personals

Personalment, la millora d'un servei en un entorn real ha estat una experiència molt enriquidora. En començar el treball i preparar les bases teòriques sobre WiFi, vaig descobrir i aprofundir en el món de la seguretat WiFi, un món que, encara que en el primer front hom hi troba el gruix de informació dedicada a poder connectar-se a Internet amb la connexió del veí, té grans apassionats i grans enginyers, programadors i matemàtics al darrera.

També val a dir que, amb la visió que dóna el pas del temps, alguns dels errors del passat en el disseny de la seguretat semblen molt greus i es podria pensar que no s'hi va treballar suficient. Potser ens hem tornat més conscients de la necessitat de la seguretat a mesura que ens han anat passant coses, i quan WiFi va sorgir la perspectiva era una altra.

Tot i així, personalment em resulta increïble que proveïdors d'accés a Internet, Telefònica la primera, segueixin incorporant WEP com a xifrat per defecte dels seus *routers*, amb unes contrasenyes que contenen un nivell d'entropia tant baix que es poden trencar en una tarda. Amb els mitjans adequats, l'obtenció d'aquestes claus és qüestió de segons (val la pena donar un cop d'ull a algunes competicions al respecte que es poden veure a YouTube).

8.4 Agraïments

Dedico aquest treball a la meva família i a tu Carla, gràcies pel teu suport incondicional. I als qui estan a prop, ells ja saben qui són. A tu Laura, per fi hem arribat! Gràcies de tot cor pel teu acompanyament i saviesa. També agraeixo l'acompanyament d'un mestre, en Marco A. Peña, en el llarg i complicat procés d'aquest TFC, de qui és un plaer aprendre una mica cada dia. I a en Quique Pérez del DTI, per acollir-me com ho ha fet.

Bibliografia

Tecnologia

1. http://www.virusprot.com/

2. http://www.inteco.es
   Estudio sobre el Sector de la Seguridad TIC en España.
   Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas.

3. Gowex: Informe Wifi 2008:
   http://www.gowex.com/noticias/tmp/informe_2008.pdf

4. http://www.ebusiness-watch.org/

5. iPass Mobile Broadband Index:
   http://www.ipass.com/pdfs/iPass_Mobile_Broadband_Index_1H_2008.pdf

6. http://www.securityfocus.com/infocus/1901/1

7. http://en.wikipedia.org/wiki/Comparison_of_wireless_data_standards

8. http://en.wikipedia.org/wiki/IEEE_802.11

9. http://www.ieee802.org/dots.html

10. Estàndards 802.11:
    http://standards.ieee.org/getieee802/802.11.html

11. http://www.embedded.com/columns/specialreports/34400002?_requestid=330456

12. http://www.windowsecurity.com/articles/80211i-WPA-RSN-Wi-Fi-Security.html

13. http://www.wireless-center.net/

14. http://forums.wi-fiplanet.com/archive/index.php/t-1293.html

15. http://www.cwnp.com/cwap/book/index.html

16. 802.11® Wireless Networks: The Definitive Guide - Matthew Gast, O'Reilly.

Auditoria

1. http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/IT_Audit_Basics/IT_Audit_Basics_Columns.htm

2. http://www.securityfocus.com/infocus/1697

3. http://searchcio.techtarget.com/sDefinition/0,,sid182_gci955099,00.html

4. http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1118060,00.html

5. http://wiki.universidadlibre.org.ar/index.php?title=%22Metodolog%C3%ADas_de_seguridad_Inform%C3%A1tica%2C_B%C3%BAsqueda_de_datos_de_un_dominio_e_IP%22

6. http://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm

7. Publicacions 800-42 I 800-115 del NIST

802.1x

1. http://www.networkworld.com/research/2002/0506whatisit.html

2. http://es.wikipedia.org/wiki/IEEE_802.1X

Seguretat

1. http://www.aircrack-ng.org/doku.php?id=links

2. http://en.wikipedia.org/wiki/Wireless_security

3. http://en.wikipedia.org/wiki/Wireless_LAN_security

4. http://hack2sec.wordpress.com/

5. http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/

6. http://www.oreillynet.com/pub/a/security/2006/03/30/what-is-wireless-security.html?page=1

7. http://techdir.rutgers.edu/wireless.html

8. http://aboba.drizzlehosting.com/IEEE/

9. http://www.securityfocus.com/infocus/1814

10. http://www.securityfocus.com/infocus/1824

11. http://altctrlsupr.net/ataques-practicos-contra-wep-y-wpa/

12. http://es.wikipedia.org/wiki/Número_pseudoaleatorio

13. http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml

14. http://lasecwww.epfl.ch/pub/lasec/doc/cha06.pdf

15. http://www.eweek.com/c/a/Security/Cracking-the-WPA-Security-Standard/1/

16. http://blogs.nuspire.com/bkblog/?p=66

17. The State of Wi-Fi® Security: Wi-Fi CERTIFIED™ WPA2® Delivers Advanced Security to Homes, Enterprises and Mobile Devices (2009) – Wi-Fi Alliance.

18. Presentació PPT: Wireless Threats and Vulnerabilities – Mischel Kwon, U.S. Department of Justice.

19. Goal-Oriented Security Threat Mitigation Patterns: A Case of Credit Card Theft Mitigation - Sam Supakkul, Tom Hill, Ebenezer Akin Oladimeji, and Lawrence Chung.

20. The Final Nail in WEP's Coffin - Andrea Bittau, Mark Handley, Joshua Lackey.

21. Practical attacks against WEP and WPA - Martin Beck, Erik Tews, 8 Novembre 2008.

22. Cryptanalysis of IEEE 802.11i TKIP - Finn Michael Halvorsen, Olav Haugen, Juny 2009.

23. A Practical Message Falsication Attack on WPA - Toshihiro Ohigashi and Masakatu Morii.

Atacs i eines

1. http://www.wireless-center.net/Wi-Fi-Security/3078.html

2. http://www.tech-faq.com/rogue-access-point.shtml

3. http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm

4. http://www.corelan.be:8800/index.php/2009/02/20/cheatsheet-cracking-wep-with-backtrack-4-and-aircrack-ng/

5. http://users.csc.calpoly.edu/~bellardo/pubs/usenix-sec03-80211dos-html/80211-dos.html

6. http://www.pcworld.com/businesscenter/article/144647/guide_to_wireless_lan_security.html

Distribucions i Eines

1. http://caballe.cat/wp/distribucions-especialitzades-en-seguretat/

2. http://kcpentrix.com/index.php?option=com_content&view=article&id=65&Itemid=71

3. http://caballe.cat/wp/distribucions-especialitzades-en-seguretat/

4. http://www.securitydistro.com/security-distros/

5. http://www.airmagnet.com/products/enterprise/

6. http://www.wi-foo.com/ViewPage80e2.html?siteNodeId=45

7. http://www.windowsecurity.com/whitepapers/Wireless-Cracking-Tools.html

8. http://sectools.org/sniffers.html

9. http://www.metageek.net/products/wi-spy-24i

10. http://www.wireless-center.net/Wi-Fi-Security/3076.html

Sistemes d'informació

1. http://es.wikipedia.org/wiki/Comparaci%C3%B3n_de_sistemas_de_monitorizaci%C3%B3n_de_redes

2. http://www.nosolounix.com/2010/04/instalar-nagios-en-ubuntu.html

3. http://www.nosolounix.com/2010/06/configurar-nagios-en-ubuntu.html

4. http://www.zenoss.com/

5. http://www.alienvault.com/community.php?section=Home

6. http://networksecuritytoolkit.org/